Journal of Competition Law & Economics, 00(00), 1–83
doi: 10.1093/joclec/nhab007

RESTRICTIONS ON PRIVACY AND EXPLOITATION IN THE DIGITAL ECONOMY: A MARKET FAILURE PERSPECTIVE

Nicholas Economides & Ioannis Lianos†*

ABSTRACT

The recent controversy on the intersection of competition law with the protection of privacy, following the emergence of big data and social media is a major challenge for competition authorities worldwide. Recent technological progress in data analytics may greatly facilitate the prediction of personality traits and attributes from even a few digital records of human behaviour. There are different perspectives globally as to the level of personal data protection and the role competition law may play in that context, hence the discussion of integrating such concerns in competition law enforcement may be premature for some jurisdictions. However, a market failure approach may provide common intellectual foundations for the assessment of harms associated with the exploitation of personal data, even when the specific legal system does not formally recognize a fundamental right to privacy. The paper presents a model of market failure based on a requirement provision in the acquisition of personal information from users of other products/services. We establish the economic harm from the market failure and the requirement using the traditional competition law toolbox and focusing more on situations in which the restriction on privacy may be analysed as a form of exploitation.

I. INTRODUCTION

The recent controversy surrounding the intersection of competition law with the protection of privacy, following the emergence of big data and social media, presents a major challenge for competition authorities worldwide. The

* Nicholas Economides is professor of economics at NYU Stern Business School and executive director of the Networks, Electronic Commerce and Telecommunications Institute. E-mail: economides@stern.nyu.edu.

† Ioannis Lianos is President of the Hellenic Competition Commission (HCC) and professor of global competition law and policy at UCL Faculty of Laws. Economides acknowledges support from NSF EARS-1547332. The authors would like to thank Megan Cochrane, Tobias Kleinschmitt, Gautam Natarajan, and Matthew J. Strader for their valuable research and editorial assistance. We also thank Eleanor Fox for comments on an earlier draft. Any errors or omissions are the authors' alone. The paper expresses personal opinions and does not represent the views of the Hellenic Competition Commission. Both authors have no conflict of interest to declare. E-mail: i.lianos@ucl.ac.uk.

concept of "big data" refers to gigantic digital datasets, which are often held by corporations, governments and other large organizations, and which can be extensively analysed using computer algorithms.[1] Breaches of privacy or data protection may affect millions of people and, depending on the purpose, even compromise the democratic process.[2]

Although tracking the number and activity of visitors to webpages has existed since the early days of the Internet, with the rise of social media and the Web 2.0, it is now technologically possible for third-party websites to be embedded into the visited website through references to external resources to the website. It can be done when a user's browser uses a JavaScript code to automatically load from the third-party server and execute.[3] Data can be harvested by digital platforms across different devices, such as smartphones, tablets, laptops and computers. It can be harvested, for instance, from websites with which the user has interacted, that is, the "first data aggregator," or from other entities, through third-party tracking with tracker harvesting data that is not directly from the user but rather is gained indirectly through access to the data aggregated by the first data aggregator. According to a study published by Ghostery in 2017, more than 77% of all page loads contain at least one tracker, for statistical or advertising purposes—Google was found to be on more than 60% of all page loads, whereas Facebook was on more than 27%, followed by Comscore, Twitter and Yandex.[4] However, it has also been reported that the implementation of stricter data protection regulation, such as the General

[1] See French Competition Authority, Autorité de la Concurrence, and German Competition Authority, Bundeskartellamt, "Competition Law and Data," (2016), Report, 4, which states that "aspects of 'big data' that are often mentioned are large amounts of different types of data, produced at high speed from multiple sources, the handling and analysis of which require new and more powerful processors and algorithms." C. Cadwalladr and E. Graham-Harrison, "Revealed: 50 Million Facebook Profiles Harvested from Cambridge Analytica in Major Data Breach," (theguardian.com, 17 March 2018), <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>, states that 'big data' is often characterized by the various 'V's, which go from four, according to certain descriptions, velocity, variety and volume, value (to be extracted) to six, according to others, with veracity and validation being adding.

[2] See the recent controversy concerning the use of Facebook generated data from Cambridge Analytica, a political strategy firm to which Facebook's clients had not provided their consent, particularly in relation to the design of algorithms that enabled Cambridge Analytical to build a system that could profile individual voters in the 2016 Brexit referendum, as well as the 2016 US Presidential election, to target them with personalized political advertisements and influence their votes. See Cadwalladr and Graham-Harrison, (1); M. Scott, "Cambridge Analytica Helped 'Cheat' Brexit Vote and US Election, Claims Whistleblower," (*politico.eu*, 27 March 2018), <https://www.politico.eu/article/cambridge-analytica-chris-wylie-brexit-trump-britain-data-protection-privacy-facebook>. There is also evidence that Google provided data on individual marginal voters to the Obama campaign of 2012.

[3] Schelter, S., Kunegis, J. 2016. Tracking the Trackers: A Large-Scale Analysis of Embedded Web Trackers, Proceedings of the Tenth International AAAI Conference on Web and Social Media.

[4] Ghostery, "Tracking the Trackers," (ghostery.com, 4 December 2017), <https://www.ghostery.com/study>

Data Protection Regulation 2016/679 (henceforth, the "GDPR"),[5] has led to a decrease in the usage of third-party cookies and third-party domains.[6] Tracking capabilities are also generally concentrated in a small number of companies, with Google holding the most power, in terms of the reach of its trackers on popular websites and apps, followed by Twitter, Facebook and Microsoft for websites trackers, and Amazon, Facebook, and Comscore for mobile app trackers.[7] The recent mergers of Microsoft/Linkedin (2016), Adobe/Lyvefire (2016), Facebook/Liverail (2014), Alibaba/Umeng (2013) and Google/Doubleclick (2007), has also contributed to the emergence of a market structure that is dominated by a small number of firms and then a long list of other less significant trackers.[8]

Furthermore, data (or information) intermediaries/ brokers, such as Axciom and Equifax, package information from various sources to profile customer groups. Historically, this profiling has helped with targeted advertising. Traditionally, advertisers build campaigns based on the following factors: geography, socio-economic status, age, government data, same-store sales and so forth. However, the internet spawned new variants of data brokers. Traditional intermediaries would collect data concerning several dimensions, such as same store sales and credit history. Combining raw purchasing history, the data for which is harvested by traditional intermediaries, with the formation of ideas, which may be done through prediction platforms (such as Facebook or Google), it may be easier to build a digital customer journey. Basic statistical models would be able to determine the optimal time to advertise to individuals to maximize conversions. In that way, payments become far more important for future advertising revenue as there will be a greater rate of conversions. Statistical models could separate window shoppers and daydreamers from serious shoppers. Although this discourse would focus largely on payments, it could be extended to encompass other decisions made by consumers.

Recent technological progress in data analytics may facilitate the prediction of personality traits and attributes, even from only a few digital records of

[5] General Data Protection Regulation (EU) 2016/679 for the protection of natural persons with regard to the processing of personal data and on the free movement of such data [2016] OJ L 119/1. This regulation came into force on 25 May 2018.

[6] Wagner, P. "News Pages Are Abandoning Third-Party Ad Trackers" (statista.com, 25 September 2018), <https://www.statista.com/chart/15578/change-of-ad-tracking-techniques-since-gdpr>, notes that in the EU third-party cookies have decreased by 22% per page while third-party domains have decreased by 4% since the GDPR came into force.

[7] Binns, R., Zhao, J., Van Kleek, M., Shadbolt, N. 2010. "Measuring Third-Party Tracker Power Across Web and Mobile," *ACM Computers in Entertainment*, 9(4): Article 39, proposes a new metric for power to measure the effect of the consolidation among tracker companies.

[8] See *ibid*; Falahrastegar, M., Haddadi, H., Uhlig, S., Mortier, R. 2014. "Anatomy of the Third-Party Web Tracking Ecosystem," *arXiv*:1409.1066.

human behaviour, such as "likes" or facial images on Facebook.[9] The inference of identities, such as an individual's social security number, from anonymised data has been possible for some time.[10] The development of smart cities, with their extensive networks of sensors and technologies, such as artificial neural networks, can serve to enable better predictions of both the actions and behaviour of smart cities' residents, or even the formation of new social ties, through better modelling and simulation.[11] Digital technology has the capacity to facilitate the elaboration of advanced, even real-time, sociometrics and new applications, such as social credit experiments.[12] These developments have brought "privacy" concerns at the forefront of the policy debate.[13]

The concept of "privacy" may be defined broadly or narrowly, and its precise contours constitute a matter of academic and non-academic discussion.[14] In view of these different conceptions of privacy in various cultures and social systems, and the heterogeneity of consumers, some of them valuing privacy highly while others much less, there are different perspectives globally as to the level of privacy protection through different legal tools, such as data protection law, or even competition law.

The emerging field of data protection, in particular in the digital sector raises interesting questions on its interaction with competition law and the need for a more connected approach between these two areas of law, as both aim to avoid the exploitation of the personal data of consumers and restrictions to their privacy,[15] even if the theoretical underpinnings of each area of law may

[9] Kosinski, M., Stillwell, D., Graepel, T. 2013. "Private Traits and Attributes are Predictable from Digital Records of Human Behaviour," *Proceedings of the National Academy of Sciences of the United States of America*, 110(15): 5802–5805.

[10] Acquisti, A., Gross, R. 2009. "Predicting Social Security Numbers from Public Data," (2009) 106(27) *Proceedings of the National Academy of Sciences of the United States of America*, 10975.

[11] See Batty, M., Axhausen, K., Giannotti, F., Pozdnoukhov, A., Bazzani, A. 2012. "Smart Cities of the Future," *The European Physical Journal*, 214:481; Almeida, A., Azkune, G. 2018. "Predicting Human Behaviour with Recurrent Neural Networks," *Applies Sciences*, 8(2):305.

[12] See Bach, J. 2020. The Red and the Black: China's Social Credit Experiment as a Total Test Environment, *British Journal of Sociology*, 71(3): 489.

[13] See, among others, Zuboff, S. 2019. *The Age of Surveillance Capitalism: the Fight for the Future at the New Frontier of Power* (Public Affairs).

[14] See, for instance, D. Solove, The meaning and value of privacy, in Roessler, B., Mokrosinska, D. (eds.), *Social Dimensions of Privacy: Interdisciplinary Perspectives* (Cambridge University Press, 2015), 71–82 (arguing that privacy is historically and culturally contingent). Privacy can be a 'final good', valued as such, or an 'intermediate good', acting as a parameter, among many, of competition: see, J. Farrell, Can Privacy be Just Another Good?, (2012) 10 Journal on Telecommunications and High Technology Law 251. While the current competition law framework may integrate the latter in defining a dimension of quality on which there may be competition (as there competition in price), the former may be more difficult to integrate in the analysis.

[15] See, 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 (March 2014); Autorité de la Concurrence & Bundeskartellamt, Competition Law and Data (16 May, 2016); US FTC, Big Data—a Tool for Inclusion or Exclusion? (January 2016) and the references included.

be different, personal data of consumers and restrictions to their privacy.[16] Indeed, data protection and privacy regulations often take a fundamental rights perspective, with privacy perceived as a rights issue.

Both the GDPR and its predecessor were inspired by a fundamental rights-based approach as both data protection and the right to privacy are protected by Articles 7 and 8 of the EU Charter of Fundamental Rights. A distinction can also be made between privacy and data, the former is formally protected and cannot be traded, whereas the latter can be traded provided the data subject has consented to such. However, no existing data protection regulation establishes a property right over personal data or confers that right to data subjects. Although the GDPR seems to be inspired by some property-like rights logic, as is evidenced by its introduction of the principles of data portability and the right to be forgotten, it stops short of recognizing property rights over data.[17] The rule is that data can be possessed by the entity collecting it without any property right being affected. As a result, platforms have been able to harvest data and, therefore, possess data without users/ data subjects retaining any property right over their data, sometimes on the basis of users consenting to the use of their data although consent is also often extracted without the user understanding the implications and the real value of this exchange, informed consent and real choice being in some cases a fiction.[18] A property right would involve providing the data subject with the use of, as well as the possibility to sell, their data, license it to someone for profit and/or use their data as security/collateral for raising capital, as is the case with intellectual property rights (henceforth, "IPRs"). Although some may consider data to be an intangible asset that may be protected by property rights, currently that is not possible with personal data.[19] The exploitation of personal data certainly creates value, however, it is entirely, or rather overwhelmingly, captured by the entities that harvest those data, such as digital platforms.

[16] See 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," (2014), Report; Autorité de la Concurrence and Bundeskartellamt, (1); US Federal Trade Commission (henceforth, 'FTC'), "Big Data—A Tool for Inclusion or Exclusion?," (2016), Report.

[17] Victor, J. 2013. "The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy," *Yale Law Journal*, 123(2): 266.

[18] For a discussion, see Bergemann, B. 2018. "The Consent Paradox: Accounting for the Prominent Role of Consent in Data Protection," in Hansen, M., Kosta, E., Nai-Fovino, I., Fischer-Hübner, S. (eds) *Privacy and Identity Management. The Smart Revolution.* (Springer), 111 (noting the need to integrate in data protection law literature a critique of power asymmetries and data subjects' dependence on digital platforms).

[19] See the discussion in Samuelson, P. 2000. "Privacy as Intellectual Property," *Stanford Law Review*, 52(5): 1125; Lessig, L. 2002. "Privacy as Property," *Social Research*, 69: 1; Schwartz, P. 2004. "Property, Privacy, and Personal Data," *Harvard Law Review*, 117: 2055; Purtova, N. 2017. "Do Property Rights in Personal Data Make Sense after the Big Data Turn? Individual Control and Transparency," *Journal of Law and Economic Regulation*, 10(2): 64.

In contrast, competition law usually takes a "market failure" approach. It is concerned with the fact that consumer or total welfare or well-being may suffer as a result of reduced data protection in the malfunctioning market for personal data acquisition, in the same way that any market could suffer from higher prices or lower quality. Additionally, although one may also envisage the possibility of a rights-based framework, to accord better with the welfarist foundations of the economic approach in competition law, the adoption of a market failure approach may arguably provide the common intellectual foundations required for the assessment of harms associated with the exploitation of personal data, even when the specific (relevant) legal system does not formally recognize a fundamental right to privacy. It may also provide the possibility of a more unified approach regarding theories of harm for both competition law and data/privacy protection. For this reason, we decide for a market failure approach, although we also recognize that there is value in protecting personal data and privacy from the perspective of fundamental rights and that, in any case, the two approaches are not mutually exclusive but may, and have already been, combined to provide the highest possible levels of protection.

We present a model of market failure based on the imposition by a company (such as Google and Facebook) on users of a requirement for the provision of personal data by such users in return for access to the products/services of the company, (henceforth, this approach is referred to as the "requirement"). In using the traditional competition law toolbox, we illustrate the economic harm suffered as a result of both the market failure and the imposition of such requirement. To eliminate both the market failure and the requirement, it is imperative to create a functioning market for the sale of personal information.

In addition to the traditional analysis undertaken regarding the requirement and the market failure, the authors note that, typically, there are informational asymmetries between the data controller and the data subject. The latter may not even be aware that their data was harvested in the first place, or that the data may be processed or shared by the data controller for a different purpose, or even sold on to third-parties. It is possible that no consent has been provided for such use, but even if there was consent for a specific use, such consent may not have extended to third-parties. The exploitation of personal data may also result from economic coercion on the basis of the user's resource-dependence or lock-in with the user having no other choice than to consent to the harvesting and use of their data, to enjoy the consumption of a specific service provided by the data controller or its ecosystem. A behavioural approach would also emphasize the possible internalities (demand-side market failures) that stem from bounded rationality and/or the fact that people do not internalize all of the consequences of their actions and face limits in their cognitive capacities. Hence, a user may consent to the harvesting and use of their data without necessarily realizing the full consequences and costs of their

choice. This may occur in the context of an exchange in which the user is offered a free product in exchange of their data.

By recognizing that there is a market failure in the acquisition and exploitation of user information, we identify a wider problem than the issue of unauthorized harvesting and use of personal data. This may result even from conduct that, at first sight, could appear as increasing consumer surplus. For instance, advertiser-based platforms, such as Google and Facebook provide free search in exchange for acquisition of private user information. Not only do these companies benefit from market power, to the extent that they control the most popular search engine and social media platforms and they have built "large 'ecosystems' of complementary products and services around their core service."[20] Furthermore, their users are locked-in since they face costs of switching to rival products.[21] Furthermore, there are considerable information asymmetries resulting out of the opaque and constantly changing data and privacy policies, as well as the fact that users are not aware of the extent of companies' surveillance.[22] In addition, these companies exploit consumers by offering a "zero price" in terms of monetary transaction for their product, although this "zero price" may be arbitrary and may underline the market failure in the acquisition of private user information. Present privacy regulations ignore this market failure as they are based on the "rights" of users but ignore that there is something fundamentally wrong with this "market" framed by these "rights."

This article is structured in the following way. Section 2 engages with the different types of market failure, before Section 3 addresses the way in which competition law has dealt with and could, in future, engage with exploitative and exclusionary conduct that results in harm to privacy. Section 4 provides some thoughts on possible remedial action beyond the strict confines of competition law. The article does not analyse other forms of user harm that may result from anti-competitive conduct pursued by platforms, such as the deterioration of the quality of search query results,[23] or the extraction of excessive prices from advertisers.[24]

[20] See, for instance, CMA, Online platforms and digital advertising—Market Study Final Report (1 July 2020), available at https://assets.publishing.service.gov.uk/media/5efc57ed3a6f4023d242ed56/Final_report_1_July_2020_.pdf, para. 56.

[21] Ibid., para. 6.45 & 59 ("platforms can use ecosystems to protect their most profitable services from competition. If platforms can convince consumers to stay within their ecosystem, a new entrant would need to compete on many fronts to displace them."

[22] Ibid., para. 5.247.

[23] See, Lianos, I., Motchenkova, E. 2013. Market Dominance and Search Quality in the Search Engine Market, *Journal of Competition Law and Economics*, 9: 419.

[24] CMA, Online platforms and digital advertising—Market Study Final Report (1 July 2020), para. 7.79.

II. PRIVACY AND MARKET FAILURES

Digital markets are affected by different types of market failure that may impact on their optimal performance with regard to delivering privacy for their users. These market failures may result from the strategies employed by large digital platforms. We present a model of market failure in the acquisition of personal information from users of other products/services of Google and Facebook arising from the requirement of these platforms that users provide their personal information if they use the company's service. We establish the economic harm from the market failure and the requirement using the traditional competition law toolbox. Eliminating the requirement and the market failure by creating a functioning market for the sale of personal information is imperative.

We also note that there are typically other types of market failures, such as consumers' lock-in, information asymmetries, missing markets enabling users to learn the value of their data, and behavioural biases. Data protection legislation offers a partial response to this exploitation of privacy and data of users, to the extent that it does not take into account, in designing its remedial strategy, all the possible long-term harms to the platforms' users, the power of some digital platforms and the "special responsibility" that may ensue from such positions of power. Competition law theories of exploitation and exclusion may thus provide a good complement to data protection law in this context.

A. Market Failures through Exclusionary and Exploitative Requirement Contracts Bundling Digital Services with Personal Data

The competition law concerns for advertising-based platforms, such Google and Facebook, are similar. Both companies allow free access to their respective services in return for the user granting them free access to their personal data/information. This information includes the specific user's IP address, cookies, location, search history and possibly, for Google, the parsing of emails and, for Facebook, the user's postings and "likes" history. Data collection by the companies occurs on a "no questions asked" basis because the default is for users to "opt-in" to the collection processes of both companies. The default opt-in and the zero price in data collection constitute a market failure. The market between the user and the company regarding the acquisition of personal data does not functions properly as a market and everyone participating in Google Internet search and/or Facebook's service is giving away their personal data for free. If the default were for users to opt-out rather than opt-in and the market for data acquisition functioned properly, users would have been able to receive various amounts of monetary compensation from these companies depending on each user's features.

Google offers free Internet search and effectively requires the provision of data from the user at zero price. It only offers Internet search *only if* the user provides their data. This setup restricts users, especially those who might be willing to pay for Google's service but would prefer not to share their personal information with the company.

The imposition of the requirement concerning the provision of personal data in return for receiving Internet search increases Google's market power in the data market. A user who would not have freely given their personal data to Google is now doing so because it is a requirement for access. As a result, this requirement increases Google's market share in the data market. Because such data are used to sell advertisements, Google's requirement directly increases its own market power, while simultaneously stifling competition, in the advertisement market. This claim is not controversial. As a recent report of the Australian Competition and Consumer Commission shows, Google and Facebook possess substantial market power in several markets, including those of online search, online advertising and news media referral in their role as "gateways" to online publications.[25]

To the extent that the users receiving free search do not receive the full level of compensation that they should for the data they provide, they are harmed by the practice resulting from the imposition of the requirement. Additionally, there are users who would prefer to pay for search but not to provide their personal data to Google. They are also harmed by being compelled to provide the personal data sought by Google's requirement.

Similarly, Facebook provides free access to its service and requires the provision of data for zero price. Facebook's service is only offered to the user if said user provides access to their personal data. Imposing a requirement concerning the provision of data to receive Facebook's services increases Facebook's market power in the data market. A user who would not have freely given their personal data to Facebook is now doing so because it is a requirement for access to the service. As a result, this requirement increases the market share of Facebook in the data market. Because the data are used to sell advertisements, Facebook's requirement directly increases its own market power, while simultaneously stifling competition, in the advertisement market. To the extent that a user is not compensated adequately for their personal data by the provision of Facebook's services for free, they will suffer damage. Additionally, users who are willing to pay Facebook for its service but would prefer not to provide their personal data to Facebook also suffer damage.

One may legitimately pose the question as what the world would be like be without this requirement. The default regime would be "opt-out" and would likely imposed by regulation, because Google, Facebook and the like, have no

[25] For an in-depth analysis of this question, see the Australian Competition and Consumer Commission (henceforth, the 'ACCC'), "Digital Platforms Inquiry," (2019), Final Report, 8–10 and 89–99.

incentive to change the present opt-in default regime. In an opt-out regime, the company, whether it be Google, Facebook or some other company, would be unable to legally use or sell the information it had collected from a user who had not opted-in. For a company to be able to use or sell information it had collected, the user would need to affirmatively give their consent to the company by opting-in. The user may demand compensation and be offered compensation for selling their data to the company. The actual opt-in could occur when a price had been determined and money had changed hands.

Ergo, a potentially vibrant market for personal information sold to companies, such as Facebook or Google, has been prevented from existing as a result of the practices pursued by Facebook and Google (and other companies) concerning the provision of personal data in return for access to their respective services. This constitutes a market failure but it can be fixed by competition authorities in the United States, the EU and other jurisdictions. This issue goes beyond privacy concerns regarding the acquisition of personal information that are typically based on the "rights" of individuals rather than the failure of markets and competition law violations.

The authors now briefly describe how the market for the sale of users' personal data may function once society departs from the arbitrarily-imposed zero pricing strategy and the present market failure.

The authors expect that there is plenty of variation regarding both a company's willingness to pay for users' personal information and users' reservation price for the sale of their personal information and users' willingness to pay for a company's service. In a competitive world, the authors would expect to see the existence of two different markets. In the case of Google, one of the two markets would be for Internet search while the other would be for the acquisition of personal data by Google. Similarly, for Facebook, there would be two separate markets. One for Facebook's social network service, and one for the acquisition of personal data by Facebook. When combining the total charges in the two markets, that is, the value collected by Google or Facebook in market one minus price paid by Google or Facebook in market two, the authors expect the following results: some users would end up paying a positive price overall, other users would be paid a positive price by the company to use that company's services, and other users would break even overall.

In addition, issues of market operation and allocative efficiency arise because of Google and Facebook's dominance in their respective markets. Even in a "default opt-out" regime, because of their market dominance, these companies can overcharge users and/or not pay them a competitive price for the provision of their personal information.

Our exposition uses Google as the dominant firm imposing the requirement, but this narrative can be easily adapted to Facebook. A user *type* may be defined by a triplet of dollar amounts (x, y, z) with variation across users in x, y, and z. We define the amount \$x as how much the user is willing to pay to use Google Internet search. That is, x is the private value/utility/consumer

surplus for Google search for the particular user and, in general, $x > 0$. We define $y as how much Google is willing to pay this particular user to induce him/her to voluntarily provide his personal data to Google (in the absence of the requirement). That is, $y is the value to Google of the personal data that the user provides to the company, and, in general, $y > 0$. We define $z as the value to the user of giving his/her private information to Google and losing his/her privacy. We will assume that $z is positive, and we will count -z as a loss for the user if his/her private data is given to the company.

We consider the following three regimes.

First, the *current requirement regime*, "opt-in," where the personal information of the user is automatically/readily available for use by the company, and the company requires personal data provision to provide Internet search.

Second, the world with *no requirement regime with competition in the personal data market*. In this world, the default is opt-out, which means that the company is not allowed to use any information gathered from the user unless the user affirmatively consents, and there is no requirement to provide personal information to access the search service. In this second regime, we assume that Google competes with other firms in search and also faces competition in the personal search market. In the latter, all rivals are very well informed on the features of the user and can practice perfect price discrimination.

In the third regime, the default is opt-out and Google is a perfectly price discriminating monopsonist in the acquisition of personal user information. It is a *no requirement regime with a perfectly price discriminating monopsonist*.

The key difference between regime 1 and regimes 2 and 3 is the imposition of the requirement contract or lack thereof. The key difference between regimes 2 and 3 is in the degree of competition among buyers in the personal information market, with regime 2 assuming competition and regime 3 assuming monopsony.

We assume that, when a user does not use search and does not provide data, he/she receives a benchmark consumer surplus normalized at zero, CS = 0. Similarly, if there is no provision of personal data by the user, Google's benefit is normalized at G = 0. We will measure changes in consumer surplus in the various actions and regime changes from these benchmarks. We assume that Google has zero marginal cost in search.[26]

We first analyse the *current requirement regime*. We have Google as a dominant firm, default "opt-in," and personal data provision is required to receive Internet search. In this regime, when the user accepts the requirement, he/she has consumer surplus

$$\mathrm{CS} = x\text{–}z,$$

as the user receives $x consumer surplus from using Google's search services and incurs a loss of personal privacy worth $z to him/her. Provided that the

[26] The marginal cost of an additional user for Google and Facebook is very low (almost zero). Most of the costs are fixed.

Table 1. Present regime: default opt-in, Google provides search only if it collects personal data

Parameter values	Actions	Benefit to user	Benefit to Google
$x > z$	User accepts the requirement, uses search and provides personal information	CS = $x - z > 0$	G = $y > 0$
$x < z$	User rejects the requirement, does not use search and does not provide personal information	CS = 0	G = 0

value from the use of Google search is higher than the user's cost of loss of privacy, $x > z$, the user accepts the requirement of Internet search to him and personal data provision to Google. Google receives an incremental benefit G equal to \$y, the value of the user's data to Google, G = y. In summary, in the present requirement regime under default opt-in, when a user accepts the requirement, the benefits to the user and Google are:

$$\text{If } x > z : \text{CS} = x\text{–}z > 0, \text{G} = y > 0.$$

If the benefit to the user from search is smaller than the cost of losing privacy, $x < z$, the user does not accept the requirement, does not use Google search, does not provide data to Google, and stays at zero consumer surplus. Google receives zero benefit as well.

$$\text{If } \; x < z : \text{CS} = 0, \text{G} = 0.$$

The current requirement regime results are summarized in Table 1.

We now change the default to opt-out and assume that data provision is not required to receive Google Internet search. In this new regime, the user uses Google Internet search, but he does not by default give the right to Google to use his personal data, even if Google collects it. Therefore, in the *no requirement regime with competition in the personal data market*, provision of personal data is a choice of the user. Google is able to charge a price p1 for Internet search and can pay price p2 to the user for personal data provision.

Rivalry among Internet search companies drives the price in the Internet search market to zero, p1 = 0,[27] resulting in

$$\text{CS} = x, \text{G} = 0$$

from the participation in the Internet search market. Because the maximum benefit from personal data to Google is y, Google would be willing to pay the

[27] If competition is less intense, price will be xk, $0 < k < 1$, with similar results.

Table 2. No requirement regime with competition in the personal data market: default opt-out, personal data provision to Google not required to provide Internet search, competition in the personal data market

Parameter values	Actions	Benefit to user	Benefit to Google
$y > z$	User provides data to Google when receiving price p2 = y	CS = $x + y - z > 0$	G = 0
$y < z$	When the user values his personal data loss more than Google values the user's data, the user does not sell his/her personal data	CS = $x > 0$	G = 0

user up to p2 = y for personal data acquisition, resulting in benefit

$$G = y\text{–}p2.$$

Once the market for personal information does not have the requirement, other firms will bid up to $y to acquire the personal information of a user. Competition among them will result in each of them offering the same price $y to the same user, resulting in zero benefit for each of them. Therefore, the user and Google benefits will be

$$CS = x\text{–}z + p2 = x\text{–}z + y, G = 0.$$

As long as the value of personal information is higher for Google than the user, $y > z$, the user prefers to accept the Google offer since then CS = $x - y + z > x$.

If it happens that $y < z$, the maximum offer a company can make to induce data provision, $y, will not be accepted by the user because it would result in lower user consumer surplus than when the user did not provide data, CS = $x + y - z < x$ because the user then had consumer surplus CS = x when not providing data. Therefore, if $y < z$, the user accepts no offer, resulting in

$$CS = x, G = 0.$$

The results of the no requirement regime with competition in the personal data market are summarized in Table 2.

In summary, the number of people who trade under no requirement with competition in the personal data market expands for some types because Google offers them a positive price to induce them to sell data, but there are also user types who participate under the requirement but do not participate without it. We explore this next.

Table 3 summarizes the differences of the two regimes.

Table 3. Comparison of the status quo with no requirement and competition in personal data market

Parameter values	Regime	Benefit to user	Benefit to Google	Participation in personal data market, in regimes 1, 2
$x > z$	Default opt-in, requirement, and user accepts Google's offer	CS = $x - z > 0$	G = $y > 0$	Yes, N/A
$z > x$	Default opt-in, requirement, and user rejects Google's offer	CS = 0	G = 0	No, N/A
$y > z$	Default opt-out, no requirement, user sells info	CS = $x + y - z > x > 0$	G = 0	N/A, Yes
$y < z$	Default opt-out, no requirement, user does not sell info	CS = x	G = 0	N/A, No
$x > z, y > z$	Change of benefit by the removal of the requirement	$\Delta CS = y > 0$	$\Delta G = -y < 0$	Yes, Yes
$x > z > y$	Change of benefit by the removal of the requirement	$\Delta CS = z > 0$	$\Delta G = -y < 0$	Yes, No
$y > z > x$	Change of benefit by the removal of the requirement	$\Delta CS = x + y - z > x > 0$	$\Delta G = 0$	No, Yes
$z > x, z > y$	Change of benefit by the removal of the requirement	$\Delta CS = x > 0$	$\Delta G = 0$	No, No

In terms of participation in the provision of data to Google, all four possibilities arise: users who accepted the requirement and also sell personal information without the requirement, users who accepted the requirement and refuse to sell without the requirement, uses who rejected the requirement and sell in its absence, and users who rejected the requirement and do not sell in its absence. [28]

[28] To understand this better, we provide examples of the four possible cases. Consider a user with $(x, y, z) = (2, 3, 1)$. Since y > z and x > z, the user participates under the requirement and also sells his/her data without the requirement. Similarly, with (3, 2, 1): $y > z$ and $x > z$ implying that the user participates under the requirement and also sells his/her data in its absence. Alternatively, consider a user with $(x, y, z) = (1, 3, 2)$. This user would not participate under the requirement since $x < z$, but would sell his/her data in its absence since y > z. Also consider user $(x, y, z) = (3, 1, 2)$. Since $x > z$, he/she would participate under the requirement, but would not sell their personal information in its absence since $y < z$. There are also those who would not participate under the requirement since $x < z$ and also would not participate in its absence since $y < z$, for example $(x, y, z) = (1, 2, 3)$ or $(2, 1, 3)$.

Several observations are in order. First, users are better off, and Google is worse off when the requirement is removed and there is competition in the personal data market, $\Delta CS > 0$, $\Delta G \leq 0$. Users are better off because they have more choice and they are not constrained by the Google-imposed requirement. Google is worse off because it can extract less surplus from the users without the compulsion of the requirement.

The second observation is that removing the requirement does not kill Google's business or its business model. There is a wide range of parameters for which users sell their personal data under no requirement, including some who would not participate in the market under the requirement but are won over by the positive price Google offers in its absence. The users who cannot be won over by Google in the absence of the requirement are only those who value their privacy more than Google values their data ($z > x, z > y$). Moreover, among those users who value their privacy more than Google values their data ($z > y$), there are some who were participating under the requirement, but having been freed from the requirement do not sell their data at prices Google are willing to offer ($x > z > y$).

The third observation is that the market for acquisition of personal data by Google works well and displays the typical features of a functioning economic market. For example, there is variation in the willingness of consumers to pay, which defines the demand curve. At any one specific price offered by Google (the buyer), some users will choose to participate in the market while others will refuse, as in most markets.

We have shown the potential for a vibrant market in the provision of personal information. Such a market is prevented from developing by Google's imposition of its requirement regarding the provision of personal data in return for access to Google's Internet search service. It is a market failure that can be fixed by the relevant competition authorities in the US, the EU and other jurisdictions.[29]

We reason that users remain worse off while Google remains better off so long as the requirement exists. Under the assumption that people can rationally determine whether it makes sense for them to provide their data, the absence of such requirement would lead to users being paid by the digital platforms for the harvesting of their data. Removing the requirement would improve consumer surplus as the price of data would be positive in its absence because users would get paid for selling their data to the platform. Typically, this would also lead to more data being collected.

We now analyse a third regime where, after opt-out, Google remains a monopsonist in the market for personal data and then compare it with regimes 1 and 2.

In this third regime, Google would be able to charge one price for search and a second price for the provision of personal data. We assume that the price

[29] The analysis for Facebook is very similar.

for search would not fully extract the benefit of search for the user, possibly because of competition between Google and its rival browsers. Thus, when the user uses Google Internet search but does not allow Google to use their personal data, the user has a benefit $x - p1$, where the price charged by Google for search only is p1 = kx, $0 \leq k \leq 1$. $k = 1$ is the special case when Google is able to extract the full benefit of the user from Internet search. It is likely that perfect price discrimination in the search market would not be possible, so it is reasonable to expect that k will be less than 1.

In this case, the consumer surplus and Google's benefit from the search market are represented by the following:

$$\text{CS} = (1\text{-k})\, x > 0 \text{ if } k < 1, \text{G} = \text{kx}.$$

All users will buy search from Google as long as $k < 1$.

Google offers payment p2 to users who are willing to sell their personal data to it. Then a user's consumer surplus and Google's benefit are:

$$\text{CS} = x\text{–}z\text{–p1} + \text{p2} = x\,(1\text{-}k)\,\text{–}z + \text{p2}, \text{G} = y + \text{kx–p2},$$

as he/she benefits from the Internet service by \$x, loses \$z for losing privacy, pays p1 = kx for search and receives p2 as monetary compensation from Google for selling his/her personal data. Google receives the personal data, which it values at y, charges p1 = kx for search and pays p2 to the user for providing that data. Therefore, the benefit to Google is $\text{G} = y + \text{kx} - \text{p2}$.

If $y > z$, that is, if the value of the user's personal data to Google is higher than the cost to the user of losing their privacy, Google can offer up to \$y and be better off than the situation in which no data is provided. Because Google is the dominant firm and can know the user so well that it can practice perfect price discrimination in the market for the provision of personal data, it will offer the lowest possible amount of money that will entice the user to provide their data, by rendering their consumer surplus slightly higher than $\text{CS} = x\,(1 - k)$, which is the level of consumer surplus when no data is provided. Therefore, Google will offer to the user, p2 = z, to buy their data. It is represented by:

$$\text{CS} = x\,(1\text{-}k)\,\text{–}z + z = x\,(1\text{–}k) > 0, \text{G} = y + \text{kx–}z > 0.$$

Note that Google's payment for personal data as a monopsonist here, p2 = z, is smaller than the amount it pays p2 = y when it faces competition in the personal data market in regime 2.

For users with $y < z$, the maximum offer Google can make to induce data provision, \$y, will not be accepted by the user because it would result in lower

user consumer surplus than when the user does not provide data:

$$CS = x\,(1-k) - z + y < x\,(1-k)\,.$$

Therefore, when y < z, the user does not provide data and the user's consumer surplus and Google benefit are

$$CS = x\,(1-k)\,, G = xk.$$

The results of the no requirement regime with Google monopsonist are summarized in Table 4a.

Table 4b compares the changes in the user's and Google's benefit across regimes 1 and 3.

Table 5 shows that competition in the personal data market will make users better off and Google worse off in comparison to Google being a monopsonist in the personal data market. It is as expected and serves to underline the fact that removing the opt-in and zero price requirement in the personal data market is not sufficient to restore the but for world.

The above analysis shows the need for strict remedies that would restore competition in the marketplace and, therefore, goes beyond the removal of the requirement.

B. Natural Monopoly or Natural Oligopoly and Market Failure in Privacy

Contrary to the repeated statements of some commentators,[30] Internet search exhibits network effects because the higher the number of search queries, the greater the quality of the search results provided by the particular search engine.[31] Thus, the more Google's market share in search increases, the greater the level of quality and value to a user of Google's search. It is a direct evidence of network effects: the higher the market share of the service, the greater value of the service to the user. Also, when the provision of data is required in return for access to search services, the more users you have, the more data you collect and, therefore, the company can sell more valuable advertisements.

[30] See Varian, H. 2017. "Use and Abuse of Network Effects," <https://www.ssrn.com/abstract=3215488> Tucker, C. "Why Network Effects Matter Less Than They Used To," (22 June 2018) *Harvard Business Review*, available at https://hbr.org/2018/06/why-network-effects-matter-less-than-they-used-to

[31] This is particularly true for idiosyncratic queries (henceforth, 'tail queries'). For a discussion, see I. Graef, *EU Competition Law, Data Protection and Online Platforms—Data as Essential Facility* (Kluwer, 2016), Section 2.4.2.

Table 4. a. No requirement, default opt-out, personal data provision to Google not required to provide Google search, Google perfectly price discriminating monopsonist in personal data market

Parameter values	**Actions**	**Benefit to user**	**Benefit to Google**
$y > z$	User provides data at price $p = z$	CS = $x\ (1 - k) > 0$	G = $y - z + \text{kx} > 0$
$y < z$	When the user values his personal data loss more than Google values the user's data, the user does not sell his/her personal data	CS = $x(1 - k) > 0$	G = xk

Table 4b. Comparison of the status quo (opt-in) to default opt-out and Google monopsonist of personal data

Parameter values	Regime	Benefit to user	Benefit to Google	Participation in personal data market, in regimes 1, 3
$x > z$	Default opt-in, requirement, and user accepts	CS = $x - z > 0$	G = $y > 0$	Yes, N/A
$z > x$	Default opt-in, requirement, and user rejects	CS = 0	G = 0	No, N/A
$y > z$	Default opt-out, no requirement, user sells info	CS = $x\ (1 - \text{k}) > 0$. When $k = 1$, CS = 0	G = $y - z + \text{xk} > \text{kx}$. When $k = 1$, G = $y - z + x > x$	N/A, Yes
$y < z$	Default opt-out, no requirement, user does not sell info	CS = $x\ (1 - \text{k}) > 0$. When $k = 1$, CS = 0	G = xk. When $k = 1$, G = x	N/A, No
$x > z, y > z$	Change of benefit by the removal of the requirement	$\Delta CS = z - \text{kx}$. When $k = 1$, $\Delta CS = z - x < 0$	$\Delta G = -z + \text{xk} < 0$. When $k = 1$, $\Delta G = -z + x > 0$	Yes, Yes
$x > z > y$	Change of benefit by the removal of the requirement	$\Delta CS = z - \text{kx} < 0$. When $k = 1$, $\Delta CS = z - x < 0$	$\Delta G = -y + \text{xk}$. When $k = 1$, $\Delta G = x - y > 0$	Yes, No
$y > z > x$	Change of benefit by the removal of the requirement	$\Delta CS = x\ (1 - \text{k})$. When $k = 1\ \Delta CS = 0$	$\Delta G = y - z + \text{kx}$. When $k = 1$, $\Delta G = x - z < 0$	No, Yes
$z > x, z > y$	Change of benefit by the removal of the requirement	$\Delta CS = x\ (1 - \text{k})$. When $k = 1\ \Delta CS = 0$	$\Delta G = \text{xk}$. When $k = 1$, $\Delta G = x > 0$	No, No

Table 5. Comparison of Google monopsonist in personal data market (regime 3) to Google in competitive personal data market (regime 2)

Parameter values	Regime	Benefit to user	Benefit to Google
$y > z$	Default opt-out, no requirement, user sells info, G monopsonist (regime 3)	CS = $x\,(1-k) > 0$. When $k = 1$, CS = 0	G = $y - z + \text{xk} > \text{kx}$. When $k = 1$, G = $y - z + x > x$
$y > z$	Default opt-out, no requirement, user sells info, personal data market competitive (regime 2)	CS = $x + y - z > x > 0$	G = 0
$y < z$	Default opt-out, no requirement, user does not sell info, G monopsonist (regime 3)	CS = $x\,(1-k) > 0$. When $k = 1$, CS = 0	G = xk. When $k = 1$, G = x
$y < z$	Default opt-out, no requirement, user does not sell info personal data market competitive (regime 2)	CS = x	G = 0
$y > z$	Change of benefit from 3 to 2 (2 minus 3)	$\Delta CS = x + y - z - x\,(1-k) = y - z + \text{xk} > \text{kx} > 0$	$\Delta G = -(y - z + \text{xk}) < -\text{xk} < 0$
$y < z$	Change of benefit from 3 to 2 (2 minus 3)	$\Delta CS = x - x\,(1-k) = \text{kx} > 0$	$\Delta G = -\text{kx} < 0$

Google's requirement concerning the provision of personal data to receive Internet search implies that as more people use Google search, Google will receive more personal data. Google uses its large market share in the market for search in combination with the imposition of its personal data requirement to increase its market share in data and, therefore, enhance its dominant position. As explained in Section 2.1, the requirement increases the ability of Google to refine its categorization of a person, which, in turn, serves to increase the amount of money that advertisers are willing to pay for such. This serves to increase its profitability.

Data collected directly from the individual user, from the location of the individual, from Google's virtual assistant, Alexa, publicly available data (for example, Census data) and data bought from data brokers are all combined by Google to refine the data that is sold directly to advertisers and/or other intermediaries. Google would not have paid for such data had it not been useful—the usefulness of this data is the complementarity it offers to make better predictions.

Size and high market share matters for advertising-based platforms, such as Google and Facebook. Firstly, the addition of a user to Google contributes to direct network effect because each addition will improve the quality of search results provided to every Google user (equally, the addition of a Facebook user will improve the Facebook experience enjoyed by all users). Additionally,

the requirement for the provision of personal data in return for receiving its Internet service serves to improve the accuracy of the data that Google and Facebook sell to advertisers and, thereby, helps increase the market share of each of these companies in the advertising market. Thus, the more users a company has using their product or services (for example, Internet search), the more the advertisers it will attract on the other side and the more valuable it is for the advertisers to use and, therefore, pay money to said company.

Traditionally "network effects" are defined as pertaining to the demand side of the market, whereas "increasing returns of scale" is a term reserved for decreasing unit cost while maintaining a consistent level of quality in production. In this context, both the scale of operation and the quality level of the company in the advertising market increase when data is provided by a greater number of users. More users who are providing their personal data under the requirement seek to reap the direct network effects in search. The requirement implies that the higher consumption levels of Google's Internet search have led to higher quality results in the advertising market. The requirement transforms a purely demand-side network effect to a supply-side effect.

With regard to advertisers and/or data brokers, Google may have monopsony power on the brokers side (in comparison to Microsoft), therefore, they can buy data more cheaply, which serves to reinforce its monopsony and monopoly with regard to advertisers.

In the previous section, the authors showed that users are worse off while Google is better off under the requirement. Assuming that people can rationally determine whether it makes sense for them to provide their data, a competitive market concerning the collection of data from users would lead to users being paid by digital platforms for the harvesting of their data. Opt-out, as opposed to default opt-in, would improve consumer surplus as the price of data would be positive and users would get paid for selling their data to the platform. This would likely lead to more data being available and collected.

There are also issues with regard to the assumption that users are able to rationally determine what is in their long-term interest, as the long-term effects of sharing data are (currently) not easy to assess. Users may be inclined to share data, particularly if they initially receive payment for it. However, they may subsequently regret selling such had they considered their long-term interests. The above could lay the foundations for a behavioural economics critique to the idea that consumers should be paid for their data and an argument that monopsony might be considered to be efficient from the perspective of social welfare.

Thus, an argument could be made for encouraging users to opt out rather than to opt for the receipt of rewards and/or positive prices for their data if they cannot determine the long-term costs of sharing their own data. Another option would be to nationalize the dominant digital platform, currently a private monopoly, and replace it with a 'public interest'-motivated monopsonist.

This would limit the harvesting of data to that which is absolutely necessary for the improvement of the service to the user and, as such, the full consumer surplus would go to the user. However, in such a scenario, innovation could end up being reduced but this could be avoided if the platform were obliged to share its data in situations in which such would lead to complementary firms developing socially useful innovations. If this were to happen, the social value of the data would outweigh the social cost of the loss of privacy to the individual user.

There is always the risk that determining that which is "socially useful" would be sub-optimal if it were done by a regulator or a state monopolist in light of the discretion offered to these bodies. This, in turn, could result in the classic criticism to the administered economy—the risk of capture and inefficiency. Hence, some other system for determining that which is socially useful may be preferable. Some authors have put forward "quadratic voting" as the procedure for overcoming the tyranny of the disinterested majority (with the majority in this scenario being those citizens who are indifferent to the protection of their privacy) and provide proportional weight to those people whose interests in a social outcome are stronger (those citizens who greatly value privacy).[32] Quadratic voting is not subject to the criticisms to the voting theory of welfare for collective decision-making to determine the "will of the people" because, unlike Arrow in his impossibility theorem[33], it does not assume ordinal preferences.

One may also refer to historical patterns in the relevant industry to assess the origins and the way in which rising concentration and dominant conduct and business strategies have harmed privacy, rather than competition on the merits, or may have reinforced the firm's dominant position by erecting important barriers to entry through the control of important amounts of data. With regard to the social media industry, Srinivasan reasons that during the time the social network market was highly competitive, with several hundreds of social networks available to users in 2007, including competing offerings from Google, Yahoo and MySpace, privacy was an important parameter of competition.[34] However, the landscape has changed significantly in recent years, predominately because of the business strategy of Facebook.

Srinivasan explains how Facebook initially entered the social media market in 2007, putting forward its "superior" privacy-centred offer, which was linked to the fact that it was a "closed communication network" that required users to join and disclose their information before being able to have access to the network, than existing dominant social networks at the time, such as MySpace. During this more competitive period, Facebook provided users

[32] Posner, E., Weyl, E. 2014. "Voting Squared: Quadratic Voting in Democratic Politics," Coase-Sandor Institute for Law and Economics Working Paper No. 657.

[33] K. Arrow, *Social Choice and Individual Values* (Wiley, 1963, First Edition, 1951).

[34] Srinivasan, D. 2019. "The Antitrust Case Against Facebook," *Berkeley Business Law Journal*, 16(1): 39.

with the ability to opt-out of having their information shared with third-parties, including advertisers and/or marketers and promised them it would remove their information on demand.[35] Any effort by Facebook to track users' behaviour, through its advertising product, Beacon, or subsequently through other social plug-in products, were unsuccessful. It led to a backlash from users. Consequently, Facebook had to withdraw its product, the Beacon, and change its privacy policies. One change involved the inclusion of a commitment to allow users to vote on future (contractual) changes that would impact upon user privacy, although the way this voting was organized raised doubts about its effectiveness.[36] However, after a decade of "false statements" and "misleading conduct" and reneging on previous promises not to track users, Facebook has been able to leverage the superior information it has over its users to sell more advertising, with the result that the market for digital advertising has been transformed to a duopoly that is dominated by Facebook and Google with the two companies accounting for 90%-99% of year-on-year growth in the U.S. digital advertising industry.[37]

Facebook also secured the co-operation of independent publishers and other businesses participating in its ecosystem to require all their businesses to "change their own privacy policies to extract, from their own users, the consent to have Facebook track them for commercial purposes."[38] More importantly, Srinivasan claims that Facebook was able to change its privacy policy towards more active user tracking, once it had beaten competing social networks with rivals, such as Snapchat and Orkut, being marginalized or excluded from the market altogether. Since then, particularly since 2014, Facebook has consolidated its dominant position on the social media market. Hence, the introduction of privacy-reducing policies were only possible because users had no other choice of social network to which they could switch and were, thus, the direct result of Facebook's dominance on the social media market.

C. Lock in and Hold up

Research focused on explaining the reasons why users would switch to a different social network from the one they currently used shows that users do not switch among social media providers on the basis of privacy reasons, rather such decisions are motivated by a number of different factors.[39] However, it should be noted that this research dates from the period before the change of the dominant business model in social media in 2014, with Facebook

[35] *Ibid*, 55–61.
[36] *Ibid*, 69.
[37] *Ibid*, 43.
[38] *Ibid*, 73.
[39] Zengyan, C., Yinping, Y., Lim, J. 2009. "Cyber Migration: An Empirical Investigation on Factors that Affect Users' Switch Intentions in Social Networking Sites," Proceedings of the 42nd Hawaii International Conference on System Sciences.

moving to its systematic monitoring and recording of users' activity, as well as the backlash and increasing awareness among users regarding the issues of privacy and personal data protection. Users may be less willing to share information on social media and are increasingly taking action to monitor their browser data and the information that they share.[40] Ad blockers have also gained in popularity. However, this has neither greatly affected the number of users switching to more privacy-centred social media nor has it led to the development of "pay-for-privacy" business models in which users pay for the service with money rather than with their data.[41] Although not centred on social media as such, the research also shows that user inertia determined by "cognitive, affective and subconscious antecedents" may also operate as a mooring factor and affect the switching behaviour of consumers.[42] Identity network effects may also have an impact upon the decision of users to switch, particularly if most of their friends are active on the platform to which they want to switch. If the user decides to switch to a rival social media platform this will result in the creation of sunk costs.[43] Such path dependency and the switching costs that arise the buyer side will likely contribute to the development of highly concentrated market structures. Single-homing is also quite prevalent in light of the development of "path dependent consumption." Users are increasingly developing consumption patterns that they are reticent to change and each additional consumption of the same product reinforces this reticence and can result in a relatively strong loyalty effect with the user being emotionally and/or subconsciously locked into a specific product or digital platform, even if the choice is not optimal, in terms of quality or the amount of personal data harvested.[44]

D. Information Asymmetries and Information-Related Failures

Under a scenario involving complete information, the user knows their valuation, $x, of Google's and Facebook's services. But is this really the current case? At present, the user does not pay for access to Google or Facebook. They

[40] Droesch, B. "How Social Media Users Have – And Have Not – Responded to Privacy Concerns, (emarketer.com, 29 April 2019), <https://www.emarketer.com/content/how-social-media-users-have-and-have-not-responded-to-privacy-concerns>.

[41] *Ibid*.

[42] Sun, Y., Liu, D., Chen, S., Wu, X., Shen, X.-L., Zhang, X. 2017. "Understanding Users' Switching Behaviour of Mobile Instant Messaging Applications: An Empirical Study from the Perspective of Push-Pull-Mooring Framework, *Computers in Human Behaviour*, 75: 727.

[43] Mahmoodi, J., Čurdová, J., Henking, C., Kunz, M., Matić, K., Mohr, P., Vovko, M. 2018. "Internet Users' Valuation of Enhanced Data Protection on Social Media: Which Aspects of Privacy are Worth the Most?," *Front Pscychol*, 9: 1516.

[44] Lee, S. 2019. "Economic Dependence on Online Intermediary Platforms and Its Exploitative Abuse," Dissertation of University of Amsterdam Law Faculty Citing Siray, S. 2016. "Combining Marketing Theory and Path Dependence," (Freie Universität Berlin), and Schulte, B. 2015. *Staying the Consumption Course—Exploring the Individual Lock-In Process in Service Relationships* (Springer).

are "free" products in terms of monetary payment. However, the user pays, that is, a cost is incurred, in providing personal data to Google or Facebook for free. This may reduce the individual user's privacy or may enable the digital platform or whoever else is controlling this data to exploit the user in the future through personalized pricing and so forth. Hence, there is an issue of transparency regarding the full costs for the user of engaging with Facebook. The user only considers the current monetary costs, which are zero; the user does not take into account future costs. Behavioural economic literature on discounting, specifically the "silver lining" effect[45] may explain why it is necessary to seriously consider behavioural biases.

The model by the authors also takes into consideration the cost of losing privacy. The user is willing to pay for Facebook, $x, but the "take-it-or leave-it" nature of Facebook's contract implies that the user will lose privacy at the cost of $z. Therefore, the net willingness of a user to pay under the present default opt-in conditions is represented by $x-$z. If the default was opt-out, the user would be willing to pay $x. In a behavioural set-up, the user may underestimate the costs of the loss of privacy.

Users do not know how much their data is valued by advertisers and/or Facebook as they have no access to the information regarding its value in the context of Facebook's transactions with advertisers and infomediaries on the other side of the platform.

Digital platforms reason that data harvesting and network effects also provide value to the users. However, the exact value of the network effects from which users (allegedly) benefit is not clear. Yet under the assumption that the data is valuable because of network effects, it is difficult to determine the value generated from data contributed by any one specific user. Regardless, the higher the number of users, the better the service and their individual data may enable the platform to provide more relevant responses to queries and improve the quality of search for tail queries. However, the issue is that if the platform collects more data than is needed for improving the service or quality of the platform this this excess harvesting of data can create a "behavioural surplus" that will in and of itself be highly valued in behavioural futures markets[46].

The lack of competition between networks results in a lack of informational transparency regarding the value of the user to the relevant digital platform, such as Facebook. As such, users are prevented from being able to negotiate a bargain for a "better" deal. The result is that there is no surplus left for users as it affects the ability of users to take collective action against the monopolist, for instance, by switching to a rival network. In any case, the choice may be quite

[45] The users are attracted by a small gain—zero price to use Facebook—and dissociate that from a large loss – been exploited in the future through perfect price discrimination.

[46] See in more detail, Zuboff, S. 2018. *The Age of Surveillance Capitalism* (Public Affairs).

limited, in view of the consolidation of the sector and the dominance of the advertisement-based model. Other issues are the broader social costs incurred as a result of the lack of individual users' knowledge regarding the harvesting of data by Facebook or Google and potential costs to democracy and pluralism. This last issue may be an important concern for both data protection and competition law in some jurisdictions.

E. Missing Markets

Previous examples of market failure assume that privacy markets do exist but operate inefficiently. However, one may decide that the problem is more fundamental than that—here there are no markets whatsoever. Contrary to the assumptions of the first fundamental theorem of welfare economics, there are no markets in which data and/or attention are demanded by companies and supplied by users, and this being traded at publicly known prices. Rather, data is harvested by search engines for free as users are not compensated for the data they contribute except for the free use of the search engine, for which, in any case, the marginal costs are close to zero. Furthermore, users cannot determine the value of their data to the digital platform as they do not have access to the information regarding the transactions on the other side of the platform between the company and the advertisers. At the same time though, users may benefit from the harvesting and use of their personal data if they are offered a more personalized service and targeted advertising, which may be positive if one adheres to the information view of advertising. The price paid by advertisers to Google or Facebook does not provide any further information as these transactions are not about users' personal raw data but about inferences made on the basis of their data.

Due to the lack of property rights on personal data, it appears that the digital economy is characterized by "missing markets."[47] Legal regimes may choose to protect entitlements to privacy or data by granting property rights by espousing liability rules and regulations, or by imposing a combination of the two. If the situation is subject to liability rules, the violation of a specific entitlement to privacy without agreement should result in compensation being paid to the victim for the damages incurred. Property rights provide their holder with the right to legally bar, by injunctive relief, anyone that violates or is likely to violate their entitlement without their consent. The underlying concept is that any property violation is severely punished by injunctive relief, which in and of itself is costly, and, thus, serves to deter the violation of any entitlement in the first place and therefore avoid future harm. Liability rules are more retrospective—they seek to provide compensation through damages for any harm incurred. Property rules facilitate the possibility of bargaining

[47] Hodgson, G. 2019. "How Mythical Markets Mislead Analysis: An Institutionalist Critique of Market Universalism," *Socio-Economic Review*, mwy049, https://doi.org/10.1093/ser/mwy049.

and they are always be more favourable to the injuree, that is, the person whose entitlement has been violated, whereas a liability rule will always be more favourable to the injurer.

Nevertheless, the allocation of property rights should not impose an externality. The imposition of an externality may occur if the provision of property rights could, for instance, lead to some users foregoing privacy in favour of instant gratification yet there may be devastating long-term consequences, not only for them personally, but also for society overall. One may envisage the social costs engendered by an entity that has induced users to freely provide or sell their personal data to manipulate them more easily. Levels of privacy protection would be reduced and, thus, greater surplus could be extracted more easily from users. As mentioned above, the lack of property rights and the consequent missing markets issue may prevent parties from negotiating a transaction that reflects Pareto efficiency. If these social costs were significant, there is also an argument for banning such transactions and, thereby, making personal data inalienable. In the authors' view, the level to which the digital economy has developed renders this a non-pragmatic option to follow at this stage.

The lack of a proper regime concerning property rights over personal data has important implications on the ability of users to protect their interests and to capture a part of the surplus value to which they contribute. Digital platforms have been able to rely on the relatively large domains of intellectual property law and contract law to impose, almost unilaterally, conditions on the users of their products. In practice, digital platforms have been able to effectively limit users' autonomy and freedom to use their tangible property as they wish. The lack of a proper property regime for personal data has enabled digital platforms to harvest this valuable raw material by merely relying on users' consent to their terms and conditions (henceforth, "Ts&Cs"); the interest of users lack protection. The possession of this data does not rely on a well-defined property regime (hence the distinction between possession and property rights) but on these digital platforms controlling important bottlenecks, specifically the way in which users can access the Internet and other various services. The GDPR does not establish a proper property rights regime for personal data. It neither grants users formal (delimited) legal rights that have been sanctioned by, and would be enforced by, a public authority, nor does it establish a system to adjudicate disputes regarding the ownership of these rights. Having possession of the item (for example, data), in the sense of physically controlling it, constitutes just one of the bundle of rights provided by property and ownership, with other expressions of the right to property being the ability to use and manage it, the right to receive income from it, the possibility to use it as capital for the production of income and the possibility to use it as security to borrow against it. It is still not possible for personal data.

III. Exploitative and Exclusionary Conduct Involving Privacy-Related Theories of Harm: *Ex Ante* and *Ex Post* Enforcement

The development of the digital economy resulted in competition authorities showing an increased level of interest in relation to privacy-related theories of harm, both in *ex ante* and *ex post* enforcement. This does not constitute an expansion of competition law field to that of other areas of law, such as data protection,[48] for the simple reason that the harm (market failure) the enforcement of competition law provisions aim to tackle is not the same as that data protection legislation gets to grips with, as the latter centres in a rights-based approach focusing on consent and does not aim to directly address the underlying market failures. Hence, one should keep in mind that competition law may go beyond the field covered by data protection legislation.[49] The authors explore the various theories submitted and the limits of existing legal tools when it comes to addressing these new theories of harm.

A. *Ex Ante* Enforcement: Data Mergers and Privacy

It is generally accepted that merger control should take into account the fact that access to personal data may constitute an important source of market power.[50] The recognition of privacy-reducing theories of harm, however, is a more complex issue particularly given the *ex ante* nature of merger control and the possibility of addressing privacy restrictions of competition *ex post* through the enforcement of data protection laws. The possibility that a merger may be considered anti-competitive because it leads to a substantial lessening of competition in relation to privacy, or more broadly may have negative consumer welfare effects because of a restriction on the level of privacy in the market, was explored in recent merger decisions in both the EU and the United States.

Digital platforms continuously add data on users and institutions. Some of the data they collect directly from the user, for example, in the default opt-in regime that we have analysed earlier. Other data they collect or buy from third parties, such as the data that Facebook collects from third party web sites if a user has a Facebook identifier and visits the third party site. Digital platforms

[48] For such a position see, Monti, G., "Attention Intermediaries: Regulatory Options and their Institutional Implications", (7 July 2020). TILEC Discussion Paper No. DP2020-018, Available at SSRN: https://ssrn.com/abstract=3646264 , at 12.

[49] See, Lianos, I. 2018. "Polycentric Competition Law," *Current Legal Problems*, 71(1): 161, 212; Deutscher, E. 2017. "How to Measure Privacy- Related Consumer Harm in Merger Analysis? A Critical Reassessment of the EU Commission's Merger Control in Data-Driven Markets" Faculty of Law, Stockholm University Research Paper No 40 <https://ssrn.com/abstract=3075200> , 33–34 (noting that "firms can lower the level of privacy protection, and thus raise the privacy-price consumers have to pay for their services without necessarily violating data protection legislation").

[50] Stucke, M., Grunes, A. *Big Data and Competition Policy* (Oxford University Press, 2016), Chapters 6–8.

additionally collect data from every aspect of life, including data from medical doctors and hospitals and from credit card companies. Recently, Google acquired Fitbit, a company that has data on exercise habits of users, thus providing it access to biometric data. Google can thus have access, not only to much more data but also data on different dimensions of one's life ("multi-modality" of data),[51] thus greatly enhancing the capacity of the platform to predict behaviour. Hence, Google is collecting data in different dimensions, creating economies of scope in data and significant learning effects, reinforcing the entrenched dominant position of the platform, both within its ecosystem, and outside. The merger has been challenged by the European Commission.[52]

As a starting point, the authors note that both the United States and the EU merger guidelines explicitly recognize non-price factors of competition.[53] In both jurisdictions, such factors may often be considered at the initial stage of market definition, rather than at the later stage of determining the relevant theories of harm. However, as a recent report of the Organisation of Economic Co-operation and Development (henceforth, "OECD") notes, "these market definition approaches have not been explicitly applied in any merger case to date."[54]

The authors here focus on the second issue as the first is relatively uncontroversial.[55] With regard to privacy concerns, the dominant view is to consider this as a parameter of competition in relation to quality. In this context it can be integrated into the competition assessment under a broadly defined "consumer welfare" standard.[56] However, this approach may be

[51] Caffarra, C., Valletti, T. Google/Fitbit review: Privacy IS a competition issue, Voxeu (4 March 2020), available at https://voxeu.org/content/googlefitbit-review-privacy-competition-issue.

[52] See, https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1446 .

[53] For the US Guidelines, see the U.S. Department of Justice (henceforth, 'DOJ') and the Federal Trade Commission (henceforth, 'FTC'), Horizontal Merger Guidelines, (2010), §4.0, which note that "enhanced market power can also be manifested in non-price terms and conditions that adversely affect customers, including reduced product quality, reduced product variety, reduced service, or diminished innovation. Such non-price effects may coexist with price effects, or can arise in their absence … when agencies investigate whether a merger may lead to a substantial lessening of non-price competition, they employ an approach analogous to that used to evaluate price competition." For the EU, see the Guidelines on the assessment of horizontal mergers under the Council Regulation on the control of concentrations between undertakings, [2004] OJ C 31/5, paras 8 ("Effective competition brings benefits to consumers, such as low prices, high quality products, a wide selection of goods and services, and innovation ") & 38.

[54] OECD. 2018. "Considering Non-Price Effects in Merger Control," Background Note by the Secretariat, DAF/COMP(2018)2, Section 112.

[55] See, for instance, the US submission to the OECD's Workshop on "Non-Price Effects of Mergers," Section 9, which notes that "evidence of the extent of direct competition between the products sold by the merger parties on non-price factors is often the same evidence relied on to determine customer substitution relevant to the hypothetical monopolist test."

[56] For a discussion, see OECD, "The Role and Measurement of Quality in Competition Analysis," (2013), DAF/COMP(2013)17. The existence of a trade-off between these various parameters of competition protected by the consumer welfare standard is an open question, particularly as "the superficial consensus" on consumer welfare "masks a deep disagreement about what 'consumer welfare' means and the best policies to promote it": G. Werden, "Consumer Welfare

subject to criticism,[57] and it should be noted that it is not the only available option.[58]

A case often mentioned with regard to the integration of privacy concerns in EU competition law is the *Facebook/WhatsApp* merger, in which a possible theory of harm explored by the EU Commission was that "the merged entity could start collecting data from WhatsApp users with a view to improving the accuracy of the targeted ads served on Facebook's social networking platform to WhatsApp users that are also Facebook users,"[59] thereby, strengthening Facebook's position in the provision of online advertising services as a result of the increased amount of data that would come under Facebook's control.[60]

However, the Commission found no concern with regard to the strengthening of Facebook's position in the online advertising service market as there was a sufficient number of alternative providers of online advertising services and a significant number of market participants that also collected user data alongside Facebook, not least Google. This competition signified (to the Commission) that a substantial and sufficient amount of Internet user data that would be valuable for the purposes of advertising remained outside of Facebook's exclusive control.[61] However, the Commission failed to give sufficient weight to the possibility that the data collected by DoubleClick, which contained information about a rich subset of the web browsing behaviour of DoubleClick's users across all publishers' websites engaged in targeted advertising, could facilitate online price discrimination and, thereby, enhance the power of the entity to exploit consumers. The Commission accepted DoubleClick's justification that it collected behavioural data from its users only for legitimate purposes, such as improving the overall experience offered to advertisers. Another jurisdiction was the fact that this aggregate data would have been of limited use because of the confidentiality clauses included in the contractual arrangements with both advertisers and publishers and the possibility of DoubleClick's customers quickly switching to alternative ad serving providers if DoubleClick were to violate any confidentiality provisions.[62] The Commission unconditionally cleared Google's acquisition of DoubleClick as it found no competition concerns on any of the relevant advertising-related markets. However, it also recognized that "it is not excluded that ... the merged entity would be able to combine DoubleClick's and Google's data collections, e.g. users' IP addresses, cookies IDs, connection times to

and Competition Policy" in *Competition Policy and the Economic Approach: Foundations and Limitations* (edited by Drexl, J., Kerber, W., Podszun, R. , Edward Elgar, 2011), 15.

[57] OECD, (55), Sections 113–19.

[58] For a discussion, see Lianos, I. 2018. "Polycentric Competition Law," *Current Legal Problems*, 71(1): 161.

[59] Facebook/Whatsapp (Case No COMP/M.7217) C(2014) 7239 final, [180].

[60] *Ibid*, [184].

[61] *Ibid*, [189].

[62] *Ibid*, [277].

correctly match records from both databases. Such combination could result in individual users' search histories being linked to the same users' past surfing behaviour on the internet (...) the merged entity may know that the same user has searched for terms A, B and C and visited pages X, Y, and Z in the past week. Such information could potentially be used to better target ads to users."[63]

However, the Commission did not focus on privacy concerns. It dismissed the possibility that the acquisition of WhatsApp by Facebook would enable Facebook to use WhatsApp users' data for the better targeting of Facebook ads—the Commission doubted whether Facebook would have both the ability and incentive to engage in such conduct post-transaction. Concerns as to the impact of the merger on privacy were also side-lined. According to the Commission, "any privacy-related concerns flowing from the increased concentration of data under 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's data protection rules."[64] The Commission focused solely on the exclusionary/anti-competitive foreclosure-related concerns. It left any possible exploitation concerns, in terms of the potential impact of the merger on users' privacy, to be dealt by the EU's data protection laws.

In August 2016, WhatsApp updated its privacy policy to allow for the phone numbers of WhatsApp users to be linked with the identity of Facebook users. Hence, the statement made at the time of the assessment of the merger proved to be untrue. Indeed, at the time the merger transaction was assessed, Facebook had offered assurances to the Commission, in the form of both a notification and a reply to a request for information, that it would be unable to establish reliable automated matching between the accounts of Facebook users and WhatsApp users. As a result of Facebook providing misleading information about the WhatsApp merger, the Commission imposed a €110 million fine on Facebook.[65] It also found that, contrary to Facebook's statements in the 2014 merger review process, the technical process of automatically matching Facebook and WhatsApp users' identities already existed in 2014, and Facebook staff were or, at least, should have been aware of such.[66] However, this did not affect the Commission's authorization of the merger as the clearance decision was based on a number of elements that went beyond automated user-matching.

In *Microsoft/LinkedIn,* the Commission raised two types of concerns/theories of harms related to data combination.[67] The first one was that the merged entity could integrate LinkedIn into Microsoft Office and, thus, combine, to the extent allowed by both contract and the applicable privacy laws, the

[63] *Ibid*, [360].
[64] *Ibid*, [164].
[65] Facebook/WhatsApp, (Case COMP/M.8228), Commission Decision (2017).
[66] *Ibid*, [86].
[67] Microsoft/Linkedin, (Case COMP M.8124), Commission Decision (2016).

user databases of both LinkedIn and Microsoft, thereby giving Microsoft the potential opportunity to shut out its competitors from the customer relationship management market. Microsoft could deny its competitors access to the LinkedIn database, which would prevent them (the competitors) from developing advanced customer relationship management functionalities through machine learning. However, the Commission was not convinced that access to the full LinkedIn database was essential to competing on the market and held that LinkedIn's product was not a "must have" solution.[68]

The second theory of harm was more directly concerned with data concentration and its possible effects on online advertising services. The Commission explored how the regulatory framework relating to data protection could mitigate some of the competition law concerns, noting that "any such data combination could only be implemented by the merged entity to the extent [that] it is allowed by applicable data protection rules [. . .]with respect to the collection, processing, storage and usage of personal data, which, subject to certain exceptions, limit their ability to process the dataset they maintain."[69] The Commission also observed that the newly adopted GDPR[70] [. . .] provides for a harmonized and high level of protection of personal data and fully regulates the processing of personal data in the EU, including *inter alia* the collection, use of, access to and portability of personal data as well as the possibilities to transmit or to transfer personal data and that "(t)his 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 (that is, easier access to personal data, right to data portability, etc.)."[71]

In light of the GDPR, the Commission found that it was not likely that in the next 2-3 years, LinkedIn data could become an important input in this market. It also found that, in any case, LinkedIn's privacy policy allowed it to share the personal data it collects, processes, stores and uses with third-parties.[72] Once again in this merger, the Commission refused to consider exploitation concerns based on the higher concentration of data and the combination of LinkedIn and Microsoft's user databases. It noted that the merger "does not raise competition concerns resulting from the possible post-merger combination of the 'data' (essentially consisting of personal information, such as information about an individual's job, career history and professional connections, and/or their email or other contacts, search behaviour and so forth) held by each of the parties in relation to online advertising."[73]

[68] *Ibid*, [400].
[69] *Ibid*, [177].
[70] GDPR, (5).
[71] Microsoft/Linkedin, (Case COMP M.8124), Commission Decision (2016) [178].
[72] *Ibid*, [255].
[73] *Ibid*, [176].

Nevertheless, the higher concentration of data could have a potential impact on competition. The Commission found that the merger could result in the marginalization of XING, a competitor of LinkedIn that offered a greater degree of privacy protection to users than LinkedIn, or it could result in making it more difficult for any potential competitor to enter into the market and would, therefore, restrict "consumer choice in relation to this important parameter of competition."[74] To address the competition concerns identified by the Commission in the professional social network services market, Microsoft offered a series of commitments. The Commission found that these commitments addressed the competition concerns identified and, because of such, it conditionally cleared the merger. This case offered the possibility of conceptualizing privacy as a parameter of competition that could eventually have been measured.[75]

Privacy-related theories of harm were also analysed in the recent merger between Apple and Shazam. This merger involved two companies that provided complementary services: software solutions platforms and digital music streaming services for Apple and music recognition apps for Shazam[76]. The Commission explored whether the fact that Shazam currently collects certain data on users of third-party apps, particularly digital music streaming apps installed on the same smart mobile devices (both Android and iOS devices) as the Shazam app, and allows those of its users who are also users of Spotify to connect their Shazam (anonymous or registered) account to their (freemium or premium) Spotify account, thereby enabling the Shazam app to identify its users. For example, the email address or Facebook identifier for registered Shazam users and the advertising identifier for anonymous Shazam users[77] could have "a negative impact on competition."[78] In assessing this element, the Commission took into account "certain legal and/or contractual limitations on the use of this customer information" by Apple post-merger.[79] Without entering into an in-depth assessment, from the perspective of data protection

[74] *Ibid*, [350]. Indeed, the Commission found that privacy was an important parameter of competition and driver of customer choice in the market for professional social networking services.

[75] Bania, K. 2018. "The Role of Consumer Data in the Enforcement of EU Competition Law," *European Competition Journal*, 14(1): 38; Deutscher E. 2017. "How to Measure Privacy-Related Consumer Harm in Merger Analysis? A Critical Reassessment of the EU Commission's Merger Control in Data-Driven Markets," Faculty of Law, Stockholm University Research Paper No. 40.

[76] Commission Decision, M.8788 - Apple/Shazam (11 November 2018).

[77] *Ibid*, [199].

[78] *Ibid*, [219].

[79] *Ibid*, [225]. The Commission refers to Article 5(1)(b) of the GDPR as indicating that "personal data which has been collected for specified, explicit and legitimate purposes may not be further processed in a manner that is incompatible with those purposes" and "data which qualifies as personal data under the GDPR can be processed by a third party only to the extent that there exists a contractual legal basis for the transmission to the third party and a legal basis for the processing by that third party"; *ibid*, [229].

law (GDPR), the Commission undertook an abridged analysis of Shazam's Ts&Cs and Privacy Notice. It concluded that the purpose for which personal data were harvested had been specified and made clear to Shazam's users. The Commission also referred to the EU rules that dealt with privacy and the protection of the confidentiality of communications, in particular the e-Privacy Directive, which may also affect the transmission of the customer information and its subsequent use.[80] However, the Commission noted that the e-Privacy Directive does not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network; therefore, it enabled Apple to lawfully store and/or have access to this customer information. Possible contractual limitations to the use of this data could emanate from the Android Developer Guidelines that had provided Shazam with access to data about the apps installed on a user's Android device, or by rivals to the new entity, such as Spotify, which, according to their developer's Ts&Cs, may restrict the use of Spotify's user data by app developers and enforce it if, post-merger, Apple would aim to collect data for services that compete with those provided by Spotify[81]. Notwithstanding these limitations, the Commission found that the new entity could collect this customer information lawfully. It then proceeded to analyse the incentive and ability of the new entity to use this user information to put its competitors at a competitive disadvantage.[82]

The *Google/Fitbit* merger could have offered the opportunity to tackle directly exploitation concerns in merger control, such as possible restrictions of privacy for the final users.[83] The Commission recognized that by acquiring Fitbit, Google would own the database maintained by Fitbit about its users' health and fitness as well as technology enabling the harvesting of data through wrist-worn wearable devices. The Commission noted that this offers a considerable data advantage in view of the increasing possibilities to "personalise" the adds Google serves through its search engine and displays on other internet pages. This was, however, assessed, only from the perspective of the possibility of Google to exclude competitors that could either compete with it in the digital healthcare sector, as well as rival wearables. To avoid a second phase investigation, Google proposed as a first set of commitments the creation of a

[80] *Ibid*, [233]-[234]. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (henceforth, the 'e-Privacy Directive'), [2002] OJ L 201/37, which, in Article 5(3), provides *inter alia* that "Member States should ensure that the storing of information or gaining access to information already stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given their consent following clear and comprehensive information about the nature of data processing

[81] *Ibid*, [237].

[82] *Ibid*, [238].

[83] Case M.9660 - Google/Fitbit (2020), currently under examination in phase 2. See, https://ec.europa.eu/commission/presscorner/detail/en/IP_20_1446 .

"data silo" in which data would be virtually stored and certain data collected through wearable devices would be kept separate from any other dataset within Google. Interestingly, this seems to also target the potential restriction of user's privacy, through the combination of different categories of data, while also trying to respond to the exclusionary concerns identified by the Commission. The Commission rejected the proposed commitments under Phase I finding that they would not cover all the data that Google would access as a result of the transaction (and valuable for advertising purposes), thus implying that the data silo remedy would not fully address its exclusionary concerns about the merger. Google suggested a new set of commitments in Phase II, which were finally accepted by the Commission. These commitments directly addressed exclusionary concerns but ignored exploitative conduct relating to privacy and did not include any specific remedy enhancing privacy, on the assumption that such issues could be successfully dealt with under the GDPR and/or the E-privacy Directive.[84]

It is surprising that exploitative concerns related to privacy did not form part of the assessment of the merger, it seems, in the humble view of the authors, on the basis of a misinterpretation of the allocation of the regulatory fields of competition law and data protection.[85] Economics has certainly the tools to analyse such exploitation concerns, either by determining the loss in quality that consumers would incur, if privacy is considered as an important dimension of quality, or by assessing the possibility that potential competition may raise the levels of privacy protection in the industry and that the merger by suppressing potential competition has a negative impact on "consumer choice" and variety (in terms of different options enabling the consumer to weigh the costs of each option to his privacy and the benefit in terms of free services or other forms of compensation he gets in exchange). Besides the issue of market failure that we have analysed earlier, a regulatory authority should assess the impact of the merger on an addition of new dimensions of data to the acquiring party or a significant enhancement of existing data, as well as the exclusion of use of such data by rivals. Thus, data acquisition should be

[84] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, [2002] OJ L 201/37.

[85] Such a misinterpretation may arise, in our view, out of the wrong assumption that the fields of data protection and competition law in this case would overlap [see, for instance Monti, G. "Attention Intermediaries: Regulatory Options and their Institutional Implications," (48)]. However, this should not be assumed. The same set of facts may lead to two different types of harm, which each area of law will assess on its own criteria of legality. We adopt the same approach regarding the *ne bis in idem* principle, with regard to what constitutes *idem*, where the same facts could give rise to different offences' unless there exist "essential elements" common to both offences (lack of identity of legal interest, see, for instance Commission Decision (COMP/39.525 – *Telekomunikacja Polska*), 22 June 2011, available at https://ec.europa.eu/competition/antitrust/cases/dec_docs/39525/39525_1916_7.pdf, paras 135-39. Why should we take a broader perspective of *idem* in this case?

analysed in its role as an enhancement of the quality of services of the merged entity and a reduction of the quality of rivals' services as a result of the merger. Regulatory authorities need to assess the extent of increasing returns to scale in the use of data by the merging parties or in the creation of exclusive network effects in the merged entity that are denied (through the merger) to rivals. These considerations may be crucial drivers of such mergers and should not be ignored.[86]

In any case, it is clear from the constitutional as well as the regulatory context in the EU regarding the preservation of privacy and data protection that these are important collective values, which the regulatory institutions put in place by the EU Treaties have the duty to protect. Hence, even the mere likelihood of a negative conflict of jurisdiction should not be tolerated, as this would amount to a dereliction of duty. It is even more problematic as the European Data Protection Board (EDPB) hinted to the privacy issues raised by this merger, noting that "(t)here are concerns that the possible further combination and accumulation of sensitive personal data regarding people in Europe by a major tech company could entail a high level of risk to the fundamental rights to privacy and to the protection of personal data."[87] In the absence of a process of regulatory cooperation between the DG Competition at the European Commission and the data protection authorities in the EU and the EDPB, and even more of a requirement of joint approval of digital mergers,[88] the Commission should step in and assess the privacy and exploitation concerns raised by the transaction, adapting if it is necessary for its own criteria to integrate privacy concerns, by eventually repurposing for the occasion concepts of data protection law.[89] This is even more necessary as

[86] Also see Peitz, M. "Economic Policy for Digital Attention Intermediaries," Zew Discussion paper No 20-035, July 2020 who advocates that Regulatory authorities should take into consideration a high price offered to a merging party as an indication of the (intangible) value of the data the party possesses.

[87] See, EDPB, Statement on privacy implications of mergers (19 February 2020), available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_2020_privacyimplicationsofmergers_en.pdf.

[88] For a very interesting discussion of the institutional dimensions of the interaction between competition law and data protection and the need for establishing mechanisms to guarantee consistency, see Monti, G. Attention Intermediaries: Regulatory Options and their Institutional Implications (7 July 2020). TILEC Discussion Paper No. DP2020-018, Available at SSRN: https://ssrn.com/abstract=3646264.

[89] This amounts to the strategy of "cross-institutional isomorphism" put forward by one of the authors of this article, which suggests that "in view of the alterity of the problem to be solved, for the specific institutional setting, it might make sense to borrow instruments and/or the overall logic from a different institutional realm and transplant them back, "repurposing them for the occasion": see, Lianos, I. 2018. "Polycentric Competition Law," *Current Legal Problems*, 71(1): 161, 200. This is subject of course to comparative institutional analysis, as the strategy may evolve, should the institutional setting change (for instance, a system of joint review of mergers or there is a requirement for the opinion of the data protection regulators). However, even in this case, as mentioned above, the harm competition law aims to tackle with regard to privacy restriction does not always coincide with what is the focus of the data protection legislation.

there is no catch-all provision in the EU for the *ex post* assessment of privacy-reducing practices, from the perspective of competition law, and the scope of Article 102 TFEU may not be sufficiently large to cover such practices if the undertaking in question does not have a dominant position on an identified relevant market.[90]

This issue takes a different dimension in the United States where harm to privacy does not come up when assessing merger activity and any privacy issues are to be dealt with through Section 5 of the Federal Trade Commission ("FTC") Act of 1914, which condemns unfair or deceptive acts or practices in or affecting commerce (ex post control).

B. *Ex Post* Enforcement: Abuse of a Dominant Position or Economic Dependence

Restrictions on privacy may also be subject to *ex post* enforcement, especially, but not exclusively, the prohibition of an abuse of a dominant position.[91]

[90] Although this last remark does not concern Google, which has been found dominant in a number of relevant markets, indeed, most of the problems relating to the "multi-modality" of data are raised by the conglomerate effects of aggregating different sources of data coming from various relevant markets on which an undertaking, or the ecosystem it controls, is active. To the extent that EU merger control, since 2004, catches all mergers that are likely to significantly impede effective competition, the scope of EU merger control is appropriately designed to analyse such aggregate effects, even if the merged entity will not acquire a dominant position in a relevant market. However, this is not the case in the context of *ex post* assessment of the business practices of such an undertaking, under Article 102 TFEU, which cannot cover conduct by the undertaking in question if it does not have a dominant position on a relevant market. This hints to the existence of a gap in the current EU competition law system with regard to privacy-reduction effects relating to conduct adopted by a undertaking in the context of an ecosystem of paramount importance for which it acts as a gatekeeper, without the undertaking in question necessarily enjoying a dominant position in a defined relevant market, even if the conduct adopted by that undertaking is likely to produce a significant impediment to effective competition.

[91] It is also possible for agreements that restrict competition on privacy to fall under the prohibition of anti-competitive collusive practices, to the extent that such an agreement will reduce competition in regard to a specific parameter, such as quality, which in some markets may be a quite significant factor. The application of this prohibition is well accepted now for agreements that restrict innovation and it should be the same for agreements that restrict privacy. To the extent that an agreement to restrict competition on privacy may not have any redeeming virtue, although its effect is certainly to reduce consumer welfare as, at least, it affects competition on quality, it is not unimaginable that a competition authority might, in future, qualify it as a restriction of competition *per se*, without any need to thoroughly assess its anti-competitive effects. However, it remains an open question as to whether agreements of this sort between undertakings with relatively low market shares, or in a non-concentrated market, may be a cause of concern capable of justifying the (rebuttable) presumption of anti-competitive effects that would result from such agreements and/or concerted practices being qualified as a restriction of competition by object. The approach currently followed by the EU courts in defining restrictions of competition by object, accepts that "the real conditions of the functioning and the structure of the market or markets in question" may be elements to take into account in assessing restrictions of competition by object: see Case C-179/16, *F. Hoffmann-La Roche Ltd and Others v Autorità Garante della Concorrenza e del* Mercato, ECLI:EU:C:2018:25, [79]-[80].

We explore different theories of harm that may give rise to competition law concerns and suggest specific tests for their assessment.

1. Excessive Data Extraction

"Excessive" data extraction may constitute a concern for some competition law regimes in the same way that excessive prices have been targeted. We first explore how excessive data extraction may compare with the excessive prices as an antitrust violation and second we examine how the methodology used to assess claims of excessive pricing may be applied to excessive data extraction antitrust claims.

2. Excessive data Extraction and Excessive Pricing: Parallels and Differences

It is worth noting that excessive pricing has been a controversial competition law issue, with certain jurisdictions, particularly the United States, that have rejected the possibility of bringing an excessive pricing case when this is solely motivated by concerns about exploitation, rather than collusion. Despite the recent extension of the scope of Section 5 of the FTC Act to some forms of hybrid excessive/exploitative practices in the context of standard setting organizations (henceforth, "SSOs") or related to standard essential patent (henceforth, "SEP") royalties, when the dominant firm has previously committed to licensing its essential proprietary technology on reasonable and non-discriminatory (henceforth, "RAND") terms,[92] or there has been a breach of the duty of good faith on a member of a SSO with regard to the standardization process,[93] U.S. antitrust law does not apply to purely exploitative practices.[94] However, in the EU (and several other jurisdictions), excessive pricing forms a well-accepted cause of action in competition law and may be found to infringe Article 102(a) of the Treaty on the Functioning of the European Union (henceforth, "TFEU").

One may reason that similar principles could apply to the excessive extraction of data. However, as Haucap explains "data is not like money"—it "does not reduce the user's ability to provide the same data to another service of multiple other services." It is "a fundamental difference to excessive pricing cases in which customers are left with less money/wealth once they have been

[92] See *Broadcom Corp. v. Qualcomm*, 501 F.3d 311 (3d Cir. 2007); *In re Robert Bosch GmbH*, File Bo 121-0081 (26 November 2012).

[93] See, *In the matter of Rambus, Inc.* (2 August 2006), Docket No. 9302, 34-35; *Rambus Inc. v. FTC*, 522 F3d 456 (DC Cir. 2008), *cert. denied*, 129 S. Ct. 1318 (2009).

[94] *Verizon Communications v.* 2004. *Law Offices of Curtis v. Trinko, LLP*, 540 U.S. 398 (often cited for such proposition). See however, First, H. 2019. Excessive Drug Pricing as an Antitrust Violation, *Antitrust Law Journal*, 82: 701 [noting that "Trinko itself was not about charging high prices (Verizon's regulated prices were actually low) but about dealing in ways that were intended to harm its competitors. Indeed, Trinko cited no cases in support of its view that charging high prices is a fine idea"].

exploited."[95] As the German competition authority, the Bundeskartellamt, noted in its recent Facebook decision, "personal data represents an unlimited commodity that is not used up by sharing and even consumers on a limited budget do not need to determine how much they are willing to pay."[96]

Nevertheless, this analysis ignores the impact that data extraction may have on privacy, specifically its reduction. Data extraction may violate the fundamental right of privacy but it may also, from a purely user surplus perspective, enable the platform to predict the preference map and, consequently, the behaviour of the user. This provides the platform with a more powerful position in its future interactions with users and enables it to reduce consumer surplus, not only in terms of not satisfying the privacy preferences of users but in also reinforcing the platform's capacity to impose different price discrimination strategies against them.[97] As the Bundeskartellamt also explains in its Facebook decision, the main problem in excessive data extraction cases is that "when consumers share their personal data, they are not really able to judge which and how much data is being collected by which company, to whom their data is being transmitted and what the implications of giving consent to data processing are."[98] Users may be unaware of the fact that the extracted data is likely to facilitate their exploitation. The issue here will, therefore, be to decide if a prophylactic intervention that focuses on excessive data extraction so as to avoid future instances of exploitation (eventually through different forms of personalized pricing and price discrimination) may be the preferred option, rather than addressing each of these instances of exploitation through the application of the relevant prohibitions on price discrimination or other forms of exploitative practices at a later stage. However, it is worth noting that this will, to some degree, require some sort of re-conceptualization of price discrimination in competition law, which is not usually prohibited *per se*.[99]

Alternatively, privacy may be considered as a personal good valued by the consumer, and, therefore, any reduction in privacy may be tantamount to a form of consumer harm, a reduction of quality. One may reason that if this is the case, the fact that the user does not switch platform, notwithstanding the excessive extraction of data, signals that, either this extraction is not considered

[95] Haucap, J. 2019. "Data Protection and Antitrust: New Types of Abuse Cases? An Economist's View in Light of the German Facebook Decision," *CPI Antitrust Chronicle*, 1.

[96] Bundeskartellamt. 2019. Facebook Decision in Administrative Proceedings, B6-22/16, <https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Entscheidungen/Missbrauchsaufsicht/2019/B6-22-16.pdf?__blob=publicationFile&v=5>, [hereinafter BKA Facebook] [571].

[97] Haucap, J. 2019. "Data Protection and Antitrust: New Types of Abuse Cases? An Economist's View in Light of the German Facebook Decision," *CPI Antitrust Chronicle*.

[98] BKA Facebook, [571].

[99] See the Robinson Patman Act of 1936 in the United States, which prohibits sellers from engaging in price discrimination, under certain conditions. In the EU, price discrimination may violate the provisions of the TFEU, essentially for considerations relating to market integration purposes.

excessive enough by the user, or that they value the services provided by the platform more than the inconvenience of reduced privacy, to the extent that the exchange is voluntary. Hence, this exchange and the "price" in terms of privacy reduction the user is ready to pay reveal his real preferences about the trade-off.

This however assumes that the user is fully informed about the reduction of their privacy and is rationally evaluating the costs and benefits of using the platform. Early studies nonetheless found that individuals will perform a "privacy calculus" before disclosing the information necessary to complete an e-commerce transaction, more recent work has shown that there is some cognitive dissonance between consumers' online behaviour, that is, their revealed preferences, and their stated preferences for privacy, which has led to the so-called "privacy paradox."[100] Users may value privacy but they may do nothing to protect it.[101] Recent research also highlights the bounded rationality of consumers when performing this privacy calculus—in other words, consumers lack the capacity to compare the costs and benefits of sharing personal information.[102] The privacy paradox is, indeed, a complex phenomenon with the apparent discrepancy of people's concerns over their privacy and their online behaviours, such as bounded rationality, cognitive biases and heuristics and/or social factors.[103] Furthermore, despite privacy notices, individuals may not always be aware of the data harvesting to which their personal information is subject as they rarely, if ever, read websites' Ts&Cs due to the length, legalistic language and the take-it-or-leave-it approach of such.[104] For want of any better alternative, "tick-click-and-hope-for-the-best" sums up most consumers' attitude. Through the Internet of Things (henceforth, the "IoT") users may, in future, allow their smart devices to engage in online transactions on their behalf based on learned preferences. A more systematic use of

[100] Acquisti, A, Taylor, R., Wagman, L. 2016. "The Economics of Privacy," *Journal of Economic Literature*, 54: 442; Benndorf, V., Normann, H.-T. 2018. "The Willingness to Sell Personal Data," *Scandinavian Journal of Economics*, 120: 1260-265; Norberg, P., Horne, D. R., Horne, D. A. 2007. "The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviours," *Journal of Consumer Affairs*, 41: 100-126.

[101] Barth, S., de Jong, M. 2017. "The Privacy Paradox – Investigating Discrepancies Between Expressed Privacy Concerns and Actual Online Behaviour – A Systematic Literature Review," *Telematics and Informatics*, 34(7): 1038.

[102] Acquisti, A., Taylor, Wagman, (94): 442-92, suggest that, often, consumers prefer short-term discounts over the long-term risk of disclosing personal information; Acquisti, A., Leslie, J., Loewenstein, G. 2013. "What is Privacy Worth?," *The Journal of Legal Studies*, 42(2): 249–274.

[103] For a literature review, see Kokolakis, S. 2017. "Privacy Attitudes and Privacy Behaviour: A Review of Current Research on the Privacy Paradox Phenomenon," *Computers and Security*, 64: 122.

[104] See, for instance, the meta-study by Mou, J., Shin, D.-H., Cohen, J. 2017. "Trust and Risk in Consumer Acceptance of E-Services," *Electronic Commerce Research*, 17(2): 255. A recent Consumer Unit and Trust Society (henceforth 'CUTS'), "User Perception Survey," (2018), Response Paper for Ministry of Electronics and Information Technology, in India that covered 2,400 respondents revealed that around 80% of users were not reading privacy policies. Key reasons were due to such policies being lengthy, the language barrier and too much legalese.

digital assistants might require default or adapted consent mechanisms.[105] Conversely, technological advances could lead to better results for consumers if, for example, artificial intelligence (henceforth, "AI") based on learned consumer patterns was used to form buyer coalitions to seek better terms.[106]

The main difficulty with excessive data extraction claims is determining that which is "excessive" and, therefore, exploitative. In a traditional excessive pricing claim, the level of prices in a competitive market (on the basis of an estimation of the level of prices from a workable competition perspective) usually serves as the counterfactual. This of course depends on the economic value of the product—it is determined either by using a "cost+" approach, which involves adding up the different costs of the product, or by comparing the price with a comparable competitive market. This latter method should be that which is preferred in the context of an intangible economy. In the case of excessive data extraction, the counterfactual may be easier to establish as the level of privacy enjoyed by the user in the absence of the specific conduct that is assessed as excessive. However, one can also imagine a more abstract counterfactual that may broadly serve as the standard by which to determine the excessive nature of the data extraction. Such would centre on the purpose of the data extraction and the way in which this affects the user's experience and, therefore, the "quality" of the service provided. One may reason that the data extracted by the platform should not be considered excessive if it is used, either to improve the product, to respond to the needs of the specific user so that the personalization is welfare-enhancing, or if, in the case of the platform employing an advertised-based model, to better match advertisers and consumers than the situation would otherwise have been. Consumers may, indeed, prefer to receive advertising that matches their preferences and informs them about the products in which they are interested rather than "junk" advertising.

Haucap observes that data extraction may be considered excessive in the presence of these two scenarios "once we assume that (a) either a sufficient number of consumers do actually receive disutility from 'excessive' data requirements and from having their data combined, or (b) consumers are somehow being harmed without noticing it."[107] Certainly, this is behaviour that may fall under data and/or consumer protection rules but as discussed in 2.3. and 2.4, the problem is exacerbated in cases in which the platform has

[105] Contissa, G., Lagioia, F., Lippi, M., Micklitz, H.-W., Palka, P., Sartor, G., Torroniet, P. 2018. "Towards Consumer-Empowering Artificial Intelligence," Proceedings of the Twenty-Seventh International Joint Conference on Artificial Intelligence Evolution of the Contours of AI, 5150–157.

[106] Some have coined the term "algorithmic consumer" to convey the complexity of the decision process in the digital era of the Internet of Things (henceforth, the 'IoT'): Gal, M., Elkin-Koren, N. 2017. "Algorithmic Consumers" *Harvard Journal of Law and Technology*, 30: 309.

[107] Haucap, J. 2019. "Data Protection and Antitrust: New Types of Abuse Cases? An Economist's View in Light of the German Facebook Decision," *CPI Antitrust Chronicle*, 1, 3.

market or bargaining power and, thus, the consumer may not easily switch to an option that is more respectful of their privacy.

This debate raises the question of "whether antitrust law should hold dominant firms to stricter data protection and privacy standards than competing firms without market power."[108] Indeed, excessive data extraction will be an issue for competition law only in situations in which a platform has a dominant position or monopoly power, or there is a collective dominant position. Smaller size platforms may, thus, be able to adopt practices of data extraction that, if they were larger, would otherwise be considered to be excessive. Some authors raise questions as to the legitimacy of such differential treatment and the higher duties imposed on dominant undertakings.

We consider that these arguments do not withstand serious scrutiny. Firstly, only dominant undertakings are targeted by legal provisions against excessive pricing; other undertakings are free to decide their pricing strategies. If this is not considered a problem in the context of excessive pricing claims, it also should not be an issue for excessive data extraction claims.

Secondly, as discussed previously, a concentrated market constitutes, from a privacy perspective, a less optimal market structure than a less concentrated market because there is a higher likelihood that the market would tip towards less-privacy centred business models, especially in light of the higher valuation by financial markets of advertisement-based platforms.

Thirdly, it is the preeminent position of the platform in its core activity and in adjacent markets that enables it to impose on its users a business model that reduces their privacy as users cannot easily, or do not generally, switch to alternative platforms that would offer higher levels of privacy protection.

Finally, non-dominant platforms are subject to data protection laws. These impose specific duties on all undertakings and data comptrollers, irrespective of their market share, to protect the privacy of their users. However, there is added value in competition law intervention.

It is therefore likely that excessive data extraction may constitute a form of exploitative behaviour if this is causally linked to a dominant position. There has indeed been some discussion over the targeting of purely exploitative behaviour through provisions concerning the abuse of a dominant position. A number of reservations were expressed concerning this issue with regard to claims of excessive pricing as well as a number of principles limiting the application of abuse of dominance provisions to purely exploitative practices under very narrow circumstances.[109] However, very few of the above criticisms apply to situations involving excessive data extraction.

[108] *Ibid*, 4.

[109] See Evans, D., Padilla, J. 2005. "Excessive Prices: Using Economics to Define Administrable Legal Rules," *Journal of Competition Law and Economics*, 1: 97; Röller, L. 2007. "Exploitative Abuses" in *European Competition Law Annual: A Reformed Approach to Article 82 EC* (edited by C. Ehlermann and M. Marquis, Hart Publishing, 2008), 525.

Firstly, although not all degrees of data extraction may be considered problematic, to the extent that data extraction may also occur in situations of perfect competition, data extraction that contravenes the threshold(s) set by data protection regulation, should such exist, can be presumed to be excessive. Upon reaching this threshold it is then a matter of analysing the specific conditions of the market on a case-by-case basis to determine whether the platform's dominant position and the data policies it has adopted have contributed to a lower level of data protection and privacy than that which would have existed in the market before said dominant firm with its dominant position emerged and data policies were altered. This case-by-case analysis of the conditions of the relevant market conditions and the firm's business strategies is commonplace in competition law analysis.

Secondly, the risk of data extraction strategies is that once they have been tried they may generate superior levels of profitability for the platforms that manage to harvest most of the personal data and, hence, could lead to increasing returns to scale and learning-by-doing, both of which may be highly valued by financial markets. Therefore, there is a risk that the mode of competition and innovation in the industry will get stuck at a suboptimal equilibrium, from the perspective of data protection. Also, the abovementioned difficulties regarding fixed costs are not that relevant in this context in view of the business strategies followed in multi-sided markets. The non-price harm to consumers, that is, the reduced privacy emerges on the advertising side of the market, which is a different market to the one on which the price effect emerges.

Thirdly, the remedies for excessive data extraction may be straightforward. In most cases, a cease and desist order would be sufficient to deal with the harm. Hence, there is no need for price regulation. Of course, if the remedy involves the requirement of charging users more for a higher privacy option, the determination of the "price" of privacy might require some form of price regulation. We explore the way in which this could be done in the last Section of this paper.

Fourthly, it is unlikely that any remedies that seek to promote data protection and user privacy will distort competition, innovation and/or R&D. On the contrary, such remedies may enable users to differentiate between the business models pursued by platforms and result in a push towards innovation efforts that promote privacy.

Fifthly, it is not clear if the problem will solve itself. Once a market has tipped to a sub-optimal equilibrium in terms of privacy, for instance if platforms that operate on the basis of the advertisement-based model of harvesting personal data dominate the market, given the importance of network effects, it could be difficult for any platform to challenge this position even if this latter platform offers a more privacy-enhancing alternative. Hence, some form of state intervention is needed.

Sixthly, determining whether a platform has extracted such an excessive quantity of data that it has violated data protection law is certainly a much easier task for the courts than determining whether a price is "excessive." The latter task involves the court undertaking sophisticated economic analysis.

One could also challenge the argument concerning the risks that such claims set for legal certainty and the argument that such claims require the development of narrow limiting principles. Contrary to situations involving price-related exploitation, courts and competition authorities would find it more easy to set clear principles on the basis of existing data protection rules, or, if such do not exist, on the basis of the hypothetical revealed preferences of consumers. These preferences can be determined either through willingness to pay (henceforth, "WTP") surveys or, because consumers usually value privacy less if they are asked how much they are willing to pay for it, instead of how much they would like to be paid to lose it (Willingness to Accept, WTA), through other methods, such as hedonic pricing.[110]

A legal test for excessive data extraction as a category of abuse of dominance There are various categories of abuse of dominance, each of them subject to a different legal test for the finding of a competition law violation.[111] The legal test for excessive pricing in the EU results from the seminal *United Brands* case in which the Court of Justice of the European Court (henceforth, the "CJEU") held that a price may be excessive if it has no reasonable relation to the economic value of the product supplied.[112] According to the CJEU, this excess could be determined by objectively calculating the difference between the selling price of the product in question and its cost of production—this would disclose the profit margin.[113] It should be noted though that some degree of profit margin would be entirely justified in dynamic industries and/or industries with network effects.

Determining a firm's profit margin would involve examining whether two cumulative conditions had been satisfied. Firstly, it would be necessary to determine "whether the difference between the costs actually incurred and the price actually charged is excessive and, if the answer to this question is in the affirmative, [secondly, it would be necessary to examine] whether a price has been imposed which is either unfair in and of itself or when compared

[110] Acquisti, Leslie and Loewenstein, (103), 268, note that "individuals' preferences for privacy may not be as stable or as internally consistent as the standard economic perspective assumes." They find that there is a "gap between privacy willingness to pay (henceforth, 'WTP') and willingness to argue (henceforth, 'WTA')." They argue "against the uncritical use of privacy valuations that have used single methods—for example, only WTP or only WTA."

[111] Lianos, I. 2009. 'Categorical Thinking in Competition Law and the Effects Based Approach in Article 82 EC, in Ezrachi, A. (ed.), *Article 82 EC: Reflections on its Current Evolution* (Hart.), 19.

[112] Case C-27/76 *United Brands v Commission* [1978] ECR 207.

[113] *Ibid*, 251.

to competing products."[114] Evidence of an excessive profit margin is not sufficient in and of itself to prove an abuse. EU competition authorities employ a cost–price approach for determining the excessive nature of a profit margin.

One option for measuring the excessive nature of prices involves (i) determining an adequate cost measure for measuring profit, that is, a "cost+" approach, (ii) comparing that measure to the price, and then (iii) assessing the excessiveness of the profit margin, which would require the definition of certain key benchmark prices. In relation to the third stage, a comparison with the prices charged by competitors might be one possible option (although one should be cautious, as price differences may indicate quality differences). In *United Brands*, the CJEU noted that "other ways may be devised— and economic theorists have not failed to think up several— of selecting the rules for determining whether the price of a product is unfair."[115] Other options have included comparing the price of the product across different geographic markets.[116] Under EU competition law, a price can be unlawfully excessive where "it bears no reasonable relation to the economic value of the product supplied." Prices can be assessed by, first, considering whether the difference between the price and the costs is excessive (henceforth, the "excessiveness limb"), and, second, whether the price was unfair either in and of itself or when compared with the price of competing products (henceforth, the "unfairness limb").[117] From an economic perspective, excessive extraction should only be of concern if it results from some form of market failure, such as a lack of competition or other barriers that would make it difficult for consumers to switch to competitors that would extract less data. However, the concept of fairness employed provides the enforcer with some leeway by which to determine broader standards.

In applying this test to the issue of excessive data extraction, Robertson reasons that "one may, in a first step, need to look at the amount of personalized data gathered through third-party tracking (i.e., the price paid by the user) and that which the user receives in return (i.e., the product's cost to the service provider and its economic value)," and from there assess "whether there is a reasonable relation between the amount of data collected that the tracker can or will carry out and the economic value of the digital service

[114] *Ibid*, 252.

[115] *Ibid*, [253].

[116] See *ibid*, [239]. Cases C-395/87 *Ministère Public v Tournier* [1989] ECR 2521 and C-110/88 *Lucazeau v SACEM* [1989] ECR 2811 both concerned the level of royalties charged by the French collecting society SACEM for the playing of recorded music in discotheques. The CJEU acknowledged that important price differentials between Member States could indicate an abuse, unless the relevant undertaking justifies the difference by reference to objective dissimilarities between the situation in the Member State concerned and the situation prevailing in all the other Member States.

[117] *Flynn Pharma Ltd and Flynn Pharma (Holdings) Ltd v Competition and Markets Authority*, [2018] CAT 11.

the users receive."[118] Alternatively, the "excessive" nature of the extraction will not be about volume of data, but about the combination of multiple data sources that may provide to the dominant undertaking the ability to predict the users' preferences map, beyond what is needed for the completion of the specific transaction or similar transactions in the future, and the harvested data that is not used to improve the quality of service to the user in the specific transaction ("data exhausts") becoming inputs to prediction algorithms and subsequently monetized in "behavioural futures markets."[119] The more intimate the personalized information held by the dominant digital platform about a user is, the more value it can extract, because, for instance, of the ability it has to sell behavioural advertising services to advertisers.

In this context, it is important to initially determine the "economic value" of the product that is, the objective value that consumers would give to the specific product in the counterfactual of a normal and sufficiently effective competitive market (that is, the "benchmark price"). However, it should be noted that the economic value of data cannot be determined in the same way as that of products and/or services in the tangible economy. The latter context involves considering the various components of the production costs (the fixed, variable and sunk costs) and a reasonable return on the costs incurred by the undertaking with respect to the relevant product.[120] As for the formulation of the counterfactual, other factors, such as barriers to entry and network effects, should also be considered.

Upon having determined the benchmark price, it would then be necessary to determine the relevant costs, which would be derived from a cost+ formula, before examining whether the difference between the price and costs in the factual, as opposed to the counterfactual, is excessive. This would then feed into the assessment of competition, which would also involve comparing the level of data extracted by the relevant platform with that extracted by other platforms in more competitive markets and/or across different customer segments, and examining the platform's own practices over a specified period of time. Any and all of these comparisons would have to be carried out on a "consistent basis" for which "objective, appropriate and verifiable criteria" would need to be employed.[121] For each and every case concerning excessive data extraction, an overall assessment should be required.

With regard to the cost+ approach, as the digital service concerns either the content or convenience provided to the user (for example, social media or

[118] Robertson, V. 2020. "Excessive Data Collection: Privacy Considerations and Abuse of Dominance in the Era of Big Data," *Common Market Law Review*, 57(1): 161.

[119] Zuboff, S. 2019. *The Age of surveillance capitalism: the fight for the future at the new frontier of power* (Public Affairs).

[120] Other ways by which to determine this value involve undertaking a comparison with other more competitive markets in which no such conduct has taken place.

[121] Case C-177/16, *Autortiesibu un komunicēšanās konsultāciju aģentūra / Latvijas Autoru apvieniba v Konkurences padome*, ECLI:EU:C:2017:689, [41] and [51].

Internet search), the cost should be related to the production of such services. However, a lot of the "free" content available on digital platforms is, in fact, produced and uploaded by users themselves. In relation to search engines, users, by providing their data, enable the platform, through learning-by-doing, to develop the analysis undertaken and operations performed by its algorithms. This development, in turn, helps the product to appeal more to the consumer.

As such, the first step of the analysis should involve some evaluation of the link between the platform's operational costs, the provision of the digital service, and any costs involved in the creation of the content, such as production costs (for example, Netflix), payment to content contributors (for example, YouTube) and so forth. Platforms may reason that data harvesting enables them to offer users targeted advertising and this should (i) be considered as welfare-enhancing and, (ii) form part of the "digital service" offered by the platform because it reduces the time and costs spent searching in comparison to the situation of across-the board advertising.[122] However, the welfare effects of targeted advertising are ambiguous and largely depend upon the specific types of personal information made available through the targeting process.[123] Furthermore, the allocation of the benefits between the advertisers, the intermediary and consumers vary and require a case-by-case assessment. If targeted advertising enhances user welfare, then any cost involved in the provision of such digital service (for instance, marketing costs) should be considered when assessing the economic value of the data. In any case, the simple fact that an undertaking earns above normal returns by harvesting more data than its competitors, if such exist, does not in and of itself prove that the level of data extracted is excessive.

As for the second step in the analysis, one should determine whether the price paid by the consumer has "no reasonable relationship" with the value of the product. This involves considering non-cost related factors on both the demand- and supply-side. From the aggregate demand curve, which indicates the maximum amount that potential customers would be willing to pay for each unit of a good, one may derive customers' marginal economic valuations for each unit.

One of the issues that may emerge in the context of excessive data extraction cases is that the "price" paid by the users either takes the form of their data, to extent of the divulgence of which to platforms (and third-party trackers) may be unknown, or their attention/ time. Users may also pay a "price" to get access to the service. There are various models concerning the monetization of digital platforms, such as providing access for free to some users while simultaneously

[122] Tucker, C. 2012. "The Economics of Advertising and Privacy," *International Journal of Industrial Organisation*, 30(3): 326.

[123] For an analysis see, Marotta, V. Zhang, K., and Acquisti, A. 2015. "The Welfare and Allocative Impact of Targeted Advertising," Thirty Sixth International Conference on Information Systems, available at https://pdfs.semanticscholar.org/62c0/6ffa2f8da2a337a555a61dc0c1803eb27448.pdf .

milking the "money market" through subscriptions, offering a free (freemium) and paid (premium) version, or an ad-supported freemium.

The third step analysis involves determining whether the amount of data harvested is "unfair," either in and of itself or in comparison to competing products. As the U.K. Competition Appeals Tribunal (henceforth, "CAT") held in *Pfizer & Flynn Pharma*, "excessiveness should not be assessed by reference to the theoretical concept of idealised or perfect competition but the real world where normal, effective competition is the most that should be expected."[124] This third step should also involve: a comparison between the level of data extracted by the platform (and its evolution) and that extracted in other comparable markets, an assessment of the differential between economic value and "price" to determine whether it is "sufficiently significant and persistent" so to be considered excessive, and consideration of any objective justification advanced by the dominant undertaking.[125]

3. *Personalized Pricing*

The practice of "behavioural pricing" or "personalised price discrimination," which is tantamount to first-degree price discrimination (or person-specific pricing), is not a mere technological possibility. Such is exhibited in the context of online commerce with its Big Data and algorithmic pricing practices illustrating that sellers can and, in fact, do charge different prices based on the specific buyer's search history or "digital shadow."[126] As such, a firm can actively manipulate consumers' choices.[127] Recent calls for intervention against this type of pricing,[128] which may be considered as a form of

[124] Flynn Pharma Ltd and Flynn Pharma (Holdings) Ltd v Competition and Markets Authority. 2018. CAT 11.

[125] *Ibid*, [443].

[126] Gal, M. 2017. "Algorithmic-Facilitated Coordination," Commission Report, DAF/COMP/WD(2017), 26, notes that "as more data is gathered about each consumer's preferences, a personalized 'digital profile' can be created by algorithms, which calculates and updates each consumer's elasticity of demand in real-time. This digital shadow can then be used by suppliers to increase their profits even further if they can price-differentiate between the offers they make to different consumers."

[127] Hanson, J., Kysar, D. 1999. "Taking Behavioralism Seriously: The Problem of Market Manipulation," *New York University Law Review*, 74: 630. For the first study of EU competition law concerning this problem, see Economides, N., Lianos, I. 2009. "The Elusive Antitrust Standard on Bundling in Europe and in the United States in the Aftermath of the Microsoft Cases," *Antitrust Law Journal*, 542.

[128] See Autorité de la Concurrence and Bundeskartellamt, (1), 21–22, which notes that, although the application of EU competition law to these practices may be debated, in Germany, the Federal Supreme Court found that the national provision against the abuse of a dominant position can include a consumer protection dimension as regards price discrimination: German Federal Supreme Court (BGH), "Entega II," KZR 5/10, judgment of 07.12.2010.For a discussion of "personalized pricing" see, Coen, P., Timan, N. 2013. "The Economics of Online Personalized Pricing," Report of the Office of Fair Trading; Oxera, "Behavioural Economics and Its Impact on Competition Policy," Report, <https://www.oxera.com/publications/behavioural-economics-and-its-impact-on-competition-policy Richards, T., Liaukonyte,

algorithmic discrimination, illustrate the broader socio-economic concerns that are raised with regard to the perceived manipulation of consumers by companies.[129] In the era of machine-learning and AI-assisted pricing, the risks of "digital" consumer manipulation may increase on an industrial scale.[130] Digital markets exacerbate the above risks because they offer "a vast psychological audit, that discovers and represents the desires of society" [131] and every individual. Digital markets offer sophisticated evaluation methods that are closely linked to the direct observation of consumer preferences but also to a more broad range of all types of preferences that have been expressed in social and private life, through the means of sociometric analysis. Big Data enable one to observe, allegedly more accurately, people's mentalities and inner desires and potentially influence the way in which people form their core preferences. This potential for large-scale manipulation given the possibilities offered by algorithms, data analysis and AI is motivating public authorities to act.

This may later feed into companies' commercial strategies, in that they may, for instance, develop personalized pricing (discriminatory) strategies. Price discrimination occurs when in two transactions in relation to two identical goods, despite both goods having the same cost, different prices are charged. "First degree price discrimination" enables producers to set individualized prices for each customer based on their knowledge of the individual's preferences.

From the commercial perspective, for price discrimination to be successful and not be defeated by consumers switching to other producers, certain conditions must exist including (i) market power, (ii) the ability to distinguish between customers, and (iii) the ability to prevent resale. Personalized pricing improves the producer's ability to distinguish between customers. It may result in both first and third degree discriminatory pricing practices deployed if, in the relevant context, it is possible for a firm to apply group pricing and therefore, discriminate, between groups of consumers. Subjecting final users to price discrimination may enable the relevant producer to capture the

J., Streletskaya, N. 2016. "Personalized Pricing and Price Fairness," *International Journal of Industrial Organization*, 44: 138; Ezrachi, A., Stucke, M. 2016. "The Rise of Behavioural Discrimination," *European Competition Law Review*, 37: 484; Ezrachi, A., Stucke, M. *Virtual Competition* (Harvard University Press, 2016), Chapter 11, which distinguishes "near perfect" discrimination, which involves the categorization of consumers through the harvesting of personal information collected with the help of Big Data and self-learning algorithms, from "behavioural" discrimination, which seeks to trigger consumer biases and increase consumption; Bourreau, M, de Streel, A., Graef, I. 2017. "Big Data and Competition Policy: Market Power, Personalized Pricing and Advertising," CERRE Project Report.

[129] Lianos, I. "Brands, Product Differentiation and EU Competition Law" in *Brands, Competition Law and IP* (edited by Desai, D, Lianos, I., Weber-Waller, S. Cambridge University Press, 2015) in which the "persuasive view" of advertising in economic literature is discussed.

[130] Calo, R. 2014. "Digital Market Manipulation," *George Washington Law Review*, 82: 995.

[131] Davies, W. *The Happiness Industry: How the Government and Big Business Sold Us Wellbeing* (Verso, 2015), 57.

entire consumer surplus and treat various individual/ groups of consumers unequally. Price discrimination may also affect competition between producers (not necessarily operating in the same relevant market) and the economy overall. Different producers compete for the limited resources/budget of both individual and groups of consumers. Due to the (first) producer being able to charge the relevant consumer the highest possible price that said consumer is willing to pay, the disposable income of the consumer, which could otherwise be used for making other purchases, is reduced and consumer welfare suffers. This suffering is particularly noteworthy when compared with the counterfactual, in which there is no digital manipulation but rather there is perfect competition and uniform pricing that is marginal cost pricing (in digital markets, this might be close to zero).

Personalized pricing or "price targeting" has been observed in various markets.[132] To the extent that this manipulation may result in welfare losses for individual consumers and/or group of consumers, it could be reasoned that these deviations from the counterfactual need to be corrected by State intervention, including the enforcement of competition law. However, this is a matter for debate. One may reason that personalized pricing should not be considered as a form of "manipulation" but as a technological opportunity to charge each consumer as much as their willingness to pay. This may, for instance, enable some consumers who would not previously have been able to purchase the specific product, if a uniform price had been implemented that was higher than their willingness to pay, to now afford the product. Personalized pricing may, therefore, have ambiguous effects on welfare, depending on the market structure and the trade-off between the "market appropriation" effect with regard to consumers with high willingness to pay and the "market expansion" effect with regard to consumers with a low willingness to pay.[133] In *Asnef-Equifax*, when examining the possible efficiency gains brought about by an information exchange that was restrictive of competition, the CJEU held that when performing the trade-off under Article 101(3) TFEU "it is the beneficial nature of the effect on *all* consumers in the relevant markets that must be taken into consideration, not the effect on *each member* of that category of consumers."[134] Hence, it seems that this assessment should be done on a general level, it should be conducted on the basis of the representative consumer of the specific relevant market.

One may also reason that the focus of EU competition law on distributive justice, particularly its emphasis on the position of consumers who would not

[132] See the analysis and examples provided in Bourreau, de Streel and Graef, (127), 40–41 and the empirical studies to which they refer.

[133] For a discussion, see Coen, P., Timan, N. 2013. "The Economics of Online Personalized Pricing," Report of the Office of Fair Trading, OFT1488; Bourreau, de Streel and Graef, (127), 43–45.

[134] Case C-238/05, Asnef-Equifax, *Servicios de Información sobre Solvencia y Crédito, SL v Asociación de Usuarios de Servicios Bancarios (Ausbanc)*, ECLI:EU:C:2006:734, [70] (emphasis added).

be worse off as a result of the specific conduct, may justify the intervention of competition law if the additional benefits from personalized pricing are not passed on to them (the consumers). This could be done either in the form of lower prices or in the form of better quality and/or innovative products. Competition law intervention may also be motivated by fairness considerations (value ethics), in particular, if personalized pricing is not transparent and, thus, consumers are not informed, or if, in light of the purpose limitation and data minimization requirements in the GDPR there is a need to limit the extensive practice by firms of algorithmic discrimination in relation to consumers' sensitive personal data.[135] These practices may also raise more conventional competition law concerns. They discourage consumers from exploring their options by making it harder and/or more expensive to return to buy after a search for alternatives, with the effect that the matching of products to consumers is sub-optimal and that consumers, on aggregate, may ultimately pay higher prices.[136]

From the perspective of competition law, there are different ways by which to deal with personalized pricing. In the EU, it is possible that such practices may be prohibited under Article 101(1)(d) TFEU or qualified as a price discrimination under Article 102(c) TFEU.[137] Article 101(1)(d) TFEU prohibits agreements that "apply dissimilar conditions to equivalent transactions with other trading parties, thereby placing them at a competitive disadvantage." Article 102(c) uses almost identical language to inhibit dominant undertakings from engaging in price discrimination. EU competition authorities have focused on price discrimination enforcement against dominant undertakings. Among the conditions for the application of this provision, there is the requirement that "other trading partners" be placed at a "competitive disadvantage." This language may suggest that this provision does not apply to discrimination against final consumers on the basis of price or other parameters of competition. However, this language has not impeded the Commission from applying Article 102(c) TFEU to final consumers in *Deutsche Post*. In this case, due to the behaviour of Deutsche Post, consumers were having to pay prices for the company's postal services that were (far) "higher than those charged to other senders and by having their mailings delayed significantly." [138] The consumers were negatively affected by the conduct of Deutsche Post. In its decision,

[135] See Art. 5(1) of the GDPR, (5); Article 9(1) of the GDPR and Section 2 of the Data Protection Act 1998, which require the "data controller," when processing personal data, to obtain specific and explicit consent to the processing of these categories of data.

[136] Armstrong, M., Zhou, J. 2016. "Search Deterrence," *Review of Economic Studies*, 83: 26.

[137] See Autorité de la Concurrence and Bundeskartellamt, (1), 21–22, which notes that, although the application of EU competition law to these practices may be debated, in Germany, the Federal Supreme Court found that the national provision against the abuse of a dominant position can include a consumer protection dimension as regards price discrimination: German Federal Supreme Court (BGH), "Entega II," KZR 5/10, judgment of 07.12.2010.

[138] Commission Decision COMP/C.1/36.915, *Deutsche Post AG*, [2001] OJ L331/40 (not appealed), [133].

the Commission noted that "Article 102 TFEU may be applied even in the absence of a direct effect on competition between undertakings on any given market. This provision may be also applied in situations where a dominant undertaking's behaviour causes damage directly to consumers."[139] It is also worth noting that the case law does not require evidence of a competitive disadvantage, which, in some cases, has been presumed.

Alternatively, personalized pricing may be challenged on the basis of Article 102(a) TFEU if it can be qualified as "directly or indirectly imposing unfair purchase or selling prices or other unfair trading conditions." For instance, it may have to the imposition of a higher price (or lower quality) than that which would have been the case (that is, the counterfactual) but for the specific digital manipulation that has, in turn, enabled the relevant producer to capture the consumer surplus in its entirety.

Should this provision be employed, it would be important to design a test with more specific conditions than just there being no reasonable relation between the price charged to the consumer and the "economic value" of the product supplied. Personalized pricing seeks to precisely set prices at the exact level that the specific consumer thinks is the economic value of the product, that is, it directly reflects the consumer's subjective perception of the products value and corresponds to its level of willingness to pay). From an economic efficiency perspective, this practice should not be considered to be problematic. However, one may reason that the "open market economy" principle of the EU Treaty[140] would require that economic value be determined by the competitive process taking place on a market, in which various actors, consumers and suppliers interact, in view of the fact that "competition is, by its very essence, determined by price."[141] Hence, the charging of a consumer a personalized price that will correspond to their willingness to pay without them being aware of this, combined with the fact that the specific consumer will be unable to benefit from the competitive process taking place on the open market and the lack information provided to the consumer to enable them to make an informed comparison with regard to the situation of other consumers may contravene "the principle of an open market economy with free competition." Such contravention would be important as one may reason that consumers value the competitive process. They do not solely value the fact that a product is within a price range that corresponds to their willingness to pay, but also that the price is essentially cultivated in the context of a market that involves continuous interactions between buyers and sellers. That said, it is necessary to explore, following a detailed comparative institutional analysis, whether competition law is the best legal instrument for

[139] Ibid, [133].

[140] TFEU, Articles 119, 120, and 127.

[141] Opinion of Advocate General Szpunar in Case C-148/15 Deutsche Parkinson Vereinigung eV v Zentrale zur Bekämpfung unlauteren Wettbewerbs eV EU:C:2016:394, [18].

dealing targeted pricing that reduces consumer welfare pricing, or if other regulatory alternatives, such as consumer protection law, data protection and privacy rules, anti-discrimination law, unfair commercial practices law and free movement law, may be more appropriate, under the specific circumstances.[142]

4. Unfair Commercial Practices and Trading Conditions

The exploitation of trading partners may take on forms other than merely higher prices. In some competition law regimes, the imposition of unfair trading conditions (henceforth, "UTCs") and/or unfair commercial practices (henceforth, "UCPs") may also constitute an abuse of a dominant position.[143] It should be noted that in such context, other legal regimes, such as those concerning unfair competition and/or contract law may also apply. The concepts of UTCs and UCPs are rather broad and non-delineated. As such, competition authorities are offered a high degree of discretion with regard to policy, while the courts are offered a high margin of interpretation through which to frame the scope of this legal category in a way they consider appropriate.

In its case law, the CJEU has held considered that contractual provisions of an "inequitable nature" may constitute an abuse, "bearing in mind both the intrinsic individual effect of those clauses and their effect when combined."[144] Similarly, the CJEU have found that contractual clauses that "make access to [a distribution] network conditional upon the firms accepting unfair terms in

[142] For a similar approach, see G. Monti, Attention Intermediaries: Regulatory Options and their Institutional Implications (7 July 2020). TILEC Discussion Paper No. DP2020-018, Available at SSRN: https://ssrn.com/abstract=3646264 . See also, Bourreau, de Streel and Graef, (127), 45–47, who note that restrictions on personalized pricing from data protection rules (the need to have the explicit consent of the data subject), consumer protection rules (disclosure to consumers regarding prices and the method by which they are calculated), unfair commercial practices (the prohibition in certain circumstances of consumer profiling and the consideration of this as a misleading commercial practice), free movement law (the prohibition of discrimination based on the service recipient's nationality or residence), as well as specific regulations on geo-blocking (see Proposal for a Regulation of the European Parliament and of the Council on addressing geo-blocking and other forms of discrimination based on customers' nationality, place of residence or place of establishment within the internal market and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC, COM(2016) 289 final), or the application of competition law provisions against geo-blocking.

[143] Article 102(a) provides as an example of abuse "directly or indirectly imposing [. . .] unfair trading conditions."

[144] Case C-127/73 *Belgische Radio en Televisie v SN SABAM and NV Fonior* [1974] ECR 313, [12]-[13].

the distribution agreement," to be abusive and that such constitute UTCs.[145] These practices need not derive directly from the contract.

Equally though, such practices may result from measures that have been unilaterally adopted by the dominant undertaking. National competition authorities have been quite active on this front, even for non-dominant undertakings.[146] Although the case law on UTCs and UCPs focuses on practices that affect other undertakings, that is, business-to-business relations (henceforth, "B2B"), there is nothing that would impede this case law from also applying to UTCs and/or UCPs that affect final consumers, that is, business-to-consumer relations (henceforth, "B2C"). This is because there is no distinction between situations in which the dominant undertaking is in competition, or not, with its trading partner downstream or upstream. Hence, the provisions that prohibit the abuse of a dominant position could also cover conduct that involves the imposition of UTCs on final consumers that would result in a reduction of quality concerning the services provided and/or other exploitative effects, such as the extraction of personal data without the user's consent.

However, this raises two questions: (i) what constitutes a UTC or UCP under EU competition law?, and (ii) how could this type of abusive conduct include non-price and privacy-related theories of harm?.

The case law does not provide clear limiting principles. Recent soft law and preparatory documents relating to the adoption of the Directive concerning unfair B2C commercial practices,[147] the Directive on unfair trading practices in B2B relationships in the food supply chain (henceforth, the "Unfair Trading Practices Directive"),[148] and the recent Platform to Business (P2B) Regulation with the aim to promote fairness and transparency for business

[145] See Case T-139/98 *Amministrazione Autonoma dei Monopoli di Stato (AAMS) v Commission* [2001] ECR II-3413, [76]; Case T-83/91 *Tetra Pak International SA v Commission* [1994] ECR II-755, [140], which was upheld in Case C-333/94 *P Tetra Pak International SA v Commission* [1996] ECR I-5951, which rendering conditional the sale of the product to the use of the dominant undertaking's repair and maintenance services, with such obligation being considered as going beyond protecting the dominant undertaking's 'commercial interest' and, thus, being disproportionate; Case T-203/01 *Manufacture Francaise des Pneumatiques Michelin v EC Commission* [2003] ECR II-4071, [141], which indicates the way in which rebate conditions that are indeterminate and non-transparent may also constitute unfair trade conditions.

[146] Renda, A., Cafaggi, F., Pelkmans, J., Correia de Brito, A. , Mustilli, F., Bebber, L. 2014. "Study on the Legal Framework Covering Business-to-Business Unfair Trading Practices in the Retail Supply Chain," Final Report.

[147] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market.

[148] See European Commission, "Unfair Trading Practices in the Business-to-Business Food and Non-Food Supply Chain in Europe," (2013), Green Paper, COM(2013) 37 final; European Commission, "Tackling Unfair Trading Practices in the Business-To-Business Food Supply Chain," (2014), Communication COM(2014) 472 final; European Commission, "Impact Assessment: Initiative to Improve the Food Supply Chain (Unfair Trading Practices)," (2018), Staff Working Document accompanying the Proposal for a Directive on Unfair Trading Practices in Business-To-Business Relationships in the Food Supply Chain, SWD(2018) 92

users of online intermediation services (henceforth, the "Intermediation Regulation"),[149] may provide a source of inspiration for this case law to develop further.

One needs to, of course, distinguish between the interpretation of Article 102 TFEU and the emergence of some aspects of EU competition law. The fact that a practice would constitute an "unfair" commercial practice under the Unfair Trading Practices Directive or the P2B Regulation, should not have an immediate bearing on the qualification of such practice as a UTC or UCP that would be prohibited under Article 102(a) TFEU. Rather, it would constitute a factual element that needs to be taken into account when interpreting the meaning of the prohibition on UTCs espoused in Article 102(a) TFEU.

Some common elements seem to define the UTC and UCP concepts in this context. The Commission has broadly defined UTCs as being "practices that grossly deviate from good commercial conduct, are contrary to good faith and fair dealing and are unilaterally imposed by one trading partner on another."[150] In defining the issue, the Commission has stated that the "transfer of excessive risk and costs to weaker parties" and/or "diminished part of added value" for the weaker party/parties may indicate an imbalance in terms of bargaining power and, thus, the existence of a UTC.[151] The overall concept, therefore, refers to value-capture practices that result in an unfair division of surplus between the actors involved.

However, the way in which the UTC and UCP concepts have so far been conceptualized in these regulatory texts is intrinsically linked to the B2B dimension of vertical competition that these rules seek to regulate as they assume that the "weaker" actor is an undertaking that takes risks rather than a final consumer. Hence, such conceptualizations may provide useful insights but certainly do not exhaust the conceptual potential of either UTCs or UCPs also in a B2C context. The German Facebook case constitutes an example of such trend.

The inability of the current case law, in the way it is interpreted, to deal with issues of unfairness in a B2B context has also led some jurisdictions to follow other directions, as the U.S. example of instituting a catch-all provision will show.

final; Directive (EU) 2019/633 on unfair trading practices in business-to-business relationships in the agricultural and food supply chain, [2019] OJ L111/59.

[149] Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services, [2019] OJ L 186/57. See also, European Commission, "Impact Assessment, Annexes," (2018), Staff Working Document accompanying the Proposal for a Regulation on Promoting Fairness and Transparency for Business Users of Online Intermediation Services, SWD(2018) 138 final; Proposal for a Regulation of the European Parliament and of the Council on promoting fairness and transparency for business users of online intermediation services, COM(2018) 238 final.

[150] European Commission, Communication, (147), 2.

[151] European Commission, Staff Working Document, (147), 11.

The German Facebook Case: Unfair Commercial Practices in a B2C Context The *Bundeskartellamt's* (BkA) (German competition authority) *case* against Facebook raises interesting issues with regard to the possible extension of Article 102 TFEU to cover abuses resulting from the exploitation of consumers by digital platforms when harvesting consumer (personal) data.[152]

Facebook merged and collected the various sources of personal data that had been generated by users of the services owned by Facebook, services like WhatsApp or Instagram (Facebook-controlled services), and merged this collection of data with that which had been generated by users of third-party websites and apps in which Facebook products, such as the "like" button and Facebook analytics, had been embedded (the Facebook third party ecosystem). The *BkA* differentiated between user data that had been generated through users using the Facebook service, and user data obtained from third-party sources that were either controlled by the Facebook corporate group, such as WhatsApp, Oculus, Masquerade and so forth, or through the use of Facebook programming interfaces on third-party websites or mobile apps (through the Facebook developer platform and Facebook Business Tools), which formed part of the broader third-party Facebook ecosystem. The *BkA considered that the latter set of user data* had not been generated through users using Facebook's social network and, as such, Facebook had not received users' consent in relation to it raising concerns with regard to a possible abuse of a dominant position. Facebook made the use of its service conditional upon the user granting the company extensive permission to use their personal data, even of that generated not on the Facebook platform but on the broader Facebook third-party ecosystem, in particular third-party websites in which Facebook Business Tools had been embedded. This exterior data collection occurred through Facebook gathering and saving user-related and device-related data from all these sources. As such, users were no longer able to control the way in which their personal data was used.

The decision focused on the infringement of German competition law, in particular of Section 19(1) of the GWB-Digitalisierungsgesetz (henceforth, the "GWB"), which prohibits unfair conduct by a dominant undertaking vis-à-vis other undertakings. The *BkA* noted that Facebook's users were oblivious as to the merging of the data and the sources from which it had been collected. They were also oblivious that the purpose of this merging was to enable Facebook to develop a detailed identity profile of users and their online activities in the broader Facebook third-party ecosystem.

In determining whether an abuse existed, the *BkA analysed* Facebook's Ts&Cs of service and its data policy. It examined whether Facebook's data processing terms were admissible in view of the principles of the harmonized European data protection rules, the GDPR. In doing so, the *BkA* indicated that a violation of EU data protection law could give rise to an

[152] BKA Facebook , (97).

abuse of a dominant position. Considering that Facebook's merging of the data constituted a violation of the users' constitutionally protected right to informational self-determination, the *BkA* decided that the specific provision of German competition law that prohibited the abusive conduct of dominant undertakings, Section 19 GWB, applied.[153] Therefore, the *BkA* seemed to establish a direct link between an infringement of competition law and an infringement of the principles concerning data protection.

The case is also interesting with regard to the definition of what constitutes a UTC and/or UCP. The *BkA* referred to past case law of the German Federal Court of Justice, which had previously stipulated that "principles from provisions of the legal system that regulate the appropriateness of conditions agreed upon in unbalanced negotiations can be used as concepts for appropriateness in the assessment of abusive practices under Section 19(1) GWB."[154] These general principles allow for quite a broad interpretation of the scope of abusive business terms (and potentially of their EU law equivalents: UTCs and/or UCPs). Hence, determining whether the business terms are abusive requires "an extensive balancing of interests... which should also take into account constitutionally protected rights."[155] According to the *BkA*, Section 19 GWB "should be applied in cases in which one contractual party is so powerful that it would be practically able to dictate contractual terms, thus, eliminating the other party's contractual autonomy."[156]

In interpreting the prohibition principle in Section 19(1) GWB, the *BkA* was inspired by the content of some of the examples of abusive conduct mentioned in Section 19(2) GWB, specifically in Sections 19(2)1 and 19(2)2 GWB. Under Section 19(2)(2), one may determine the abusive nature of trading conditions and/or commercial practices by comparing business terms "which differ from those which would very likely arise if effective competition existed"—this can be done by taking into account the conduct of undertakings in comparable markets in which effective competition exists. However, this is not the only way to determine the abusive and unfair nature of business terms and trading conditions. The *BkA* also made use of the broader "appropriateness principle" which "is based on constitutional values, the principles of the legislation on unfair contract terms and other civil law general clauses."[157] The aim is to preserve the "constitutionally protected right to self-determination in business affairs, i.e., commercial freedom, because the other party is able to *unilaterally* determine the terms of the contract."[158] This unilateralism in relation to the determination of contractual conditions runs contrary to the usual assumption in contract law regarding the existence of a mutually

[153] *Ibid*, [523].
[154] *Ibid*, [526].
[155] *Ibid*.
[156] *Ibid*.
[157] *Ibid*, [528].
[158] *Ibid*.

beneficial agreement based on consent and a meeting of minds. It leans toward the fact that the transaction in question may be better described as being an "uncontract".[159] By doing so, the *BkA* took a broad view of the concept of "abusive business terms".[160]

The reasoning the *BkA* undertook is also interesting as to the relation between harm to competition (competition law) and harm to data protection (data protection law). As a first step in its approach it acknowledged that Facebook's Ts&Cs and data policies constitute a violation of the GDPR's data protection values.[161] It proceeded to undertake a very detailed analysis of the GDPR framework and the possible justification that Facebook could have submitted in the data protection law assessment. The *BkA* noted that the need to process data collected from other Facebook-owned services or third-parties was not necessary for the performance of the contract with the Facebook user, the contents of which are unilaterally imposed on the data subject by the data controller. Hence, one needs to thoroughly examine the existence of voluntary consent in relation to the processing of data.

This is even more so for the data harvested by Facebook in the context of its third-party ecosystem. The *BkA* rejected Facebook's argument that the data processing was necessary for contractual purposes as it enabled users to enjoy a more personalized user experience and helped improve the quality of the service to users. The *BkA* noted that "this view means the company would be entitled to unlimited data processing solely on the grounds of its business model and product properties as well as the company's idea of product quality," something which it categorically rejected.[162] In light of the quantities of data collected by Facebook, the *BkA* considered that Facebook could have achieved a high degree of personalization solely on the basis of the data generated from the Facebook website itself.[163] This statement from the *BkA* is particularly interesting as it may constitute an argument that may also be relevant in the context of excessive data extraction claims. It would neutralize the argument that is frequently submitted by digital platforms that data extraction is not excessive to the extent that it improves the quality of the product, for instance, through increased personalization. One may doubt the effectiveness of this argument as increased personalization may lead to instances of future exploitation rather than just facilitating targeted advertising. As the *BkA* noted, "another particularly problematic aspect" of such data processing is that the aggregation of data across Facebook-owned and third party websites enables "active fingerprinting" and the "detailed profiling" of users, which "leads to a massive additional invasion of privacy, since profiling

[159] Zuboff, S. *The Age of surveillance capitalism: the fight for the future at the new frontier of power* (Public Affairs, 2019).
[160] *Ibid*, [534].
[161] *Ibid*, [573] et seq.
[162] *Ibid*, [692].
[163] *Ibid*, [744].

tracks the affected users via an immense number of websites and apps, and the captured data is combined both with the data from Facebook-owned services and with the Facebook user data."[164]

Although the *BkA* made efforts to interpret the relevant provisions of the GDPR according to data protection law, it is remarkable that it frequently referred to and used analogical reasoning when interpreting the GDPR with regard to competition law. For instance, it challenged Facebook's claim that the aggregation of this data across the various websites owned by Facebook aimed to promote the "consistency of the user experience." The *BkA* considered that the integration of services and/or functionalities along with the sharing of user data "is problematic under competition law" given the leveraging or maintenance of market power concerns that this may raise. It was also problematic because it provided the company with the possibility of excluding other market players, creating barriers to new entrants and enhancing the lock-in effect by making it more difficult to switch to other providers.[165]

In exploring the compatibility of Facebook's practices with the GDPR, the *BkA* took into account the legitimate interests of the affected stakeholders, specifically third-parties, such as advertisers that want to buy targeted advertising from Facebook, and Facebook users. The German competition authority framed the issue as one that relates to the protection of citizens' constitutionally protected right to "informational self-determination."[166] The *BkA* could have also focused on the quality dimension of competition and the fact that it had been reduced by users no longer being able to control the way in which their personal data was. However, it made no effort to build such a quality narrative based on this "loss of control". The reason for its exclusion was simply because the *BkA* would have had to explain why users had not switched to different social networks if informational self-determination was a parameter of quality competition. For this to happen, the price revealed preference, or the contingent valuation method, would have required some analysis concerning substitutability between social networks that respect informational self-determination and those, like Facebook, that violated this principle be undertaken. Instead of doing this, the evidentiary basis on which the *BkA* has built its theory of harm seems to relate more to citizens' right to informational self-determination/privacy as these are espoused and protected by both the German constitution and data protection law.

In essence, the *BkA* balanced the right of self-determination for Facebook users with the right of entrepreneurial freedom for Facebook. In doing so, it noted that the legitimate commercial interests of Facebook cannot outweigh those of Facebook's users, particularly as the data processing was not necessary and in view of the broader harms and disadvantages that such processing

[164] *Ibid*, [847].
[165] *Ibid*, [747]-[749].
[166] *Ibid*, [760].

would impose on the data subjects, in particular for certain sets of sensitive data, type of data processing, the data subjects' reasonable expectations and the position of the data controller.[167] This balancing of interests was performed in relation to the processing of data harvested from the services owned by Facebook, as well as in relation to the data collected through third-party websites and apps in which Facebook Business Tools were embedded (Facebook third-party ecosystem). Both balancing assessments arrived at similar conclusions—the rights of users outweigh those of Facebook and other third parties.[168]

By finding that the GDPR-based justifications for Facebook's conduct did not apply because of the gross imbalance between the interests of Facebook, only some of which are legitimate, and the protection of users' fundamental rights, the *BkA* concluded that the principles of the GDPR had been infringed. However, this did not automatically result in there being a competition law infringement. In the second step of the analysis, the *BkA* undertook a competition law assessment of this conduct analysing the way in which the infringement of data protection could be abusive under Section 19(1) GWB. This analysis is comprised of two parts. First, the *BkA* examined whether there was some causal link between Facebook's market power and the abusive data processing conditions it imposed on its users. Second, it sought to balance the competing interests under competition law.

In performing the first part of the test the BkA adopted a rather flexible understanding of the "causal link" concept. According to the *BkA*, "the required link with market power is, therefore, not to be construed within the meaning of a strict causality of market power, requiring proof that data processing conditions could be formulated in such a way precisely and solely because of market power."[169] Causality is, thus, perceived from a normative perspective, as a causality in relation to the outcome, rather than as a causality in the form of a strict counterfactual or but-for test that aims to determine the single, most important causal factor.[170] Although this does not mean, at least on a conceptual level, that this step of the competition analysis completely merges with the analysis undertaken in regard to data protection law, in practice it is unclear how the two may refer to different issues. Hence, it is now decided, as a matter of data protection *and* competition law that "companies behaving in a similar way that do not have a dominant position in the market would need to be assessed differently" from undertakings with market power.[171] Notwithstanding the existence of a normative causal link, the *BkA* also considered that there was a strict causality between the data policies that it found to be problematic and Facebook's dominant position—the firm's

[167] *Ibid*, [767].
[168] *Ibid*, [836].
[169] *Ibid*, [873].
[170] *Ibid*, [873] and [875].
[171] *Ibid*, [879] and [882].

market power correlated to some extent to its violation of data protection law.[172]

The second part of the test involves balancing the various interests, this time under the guise competition law, taking into account the objective of the German competition Act to promote free competition. However, as the *BkA* held that if the terms of business violate data protection values *as a result of* market power, then the balancing of interests under competition law has no "independent significance" to that undertaken in relation to data protection law. This, effectively creates a presumption of anti-competitive effects if data protection law has been violated and there is evidence of some causal link between it and market power. This latter factor, as was indicated in the above paragraph can be satisfied by the mere existence of some simple correlation. However, this did not impede the *BkA* from undertaking such a (precautionary) balancing exercise in this case, although it did note that in this case it led "to the same outcome as the balancing of interests under data protection law."[173]

According to the *BkA*, the need for an independent additional balancing under competition law is challenged by the case law of the Federal Court of Justice, which has historically emphasized that "if an infringement (of data protection law) is the result of market power ... the abusiveness can no longer be called into question by a further (competition) balancing of interests."[174] This rather blunt observation hints at the possibility that the *BkA applies* a presumption of illegality under competition law in relation to conduct that infringes data protection law provided there is some evidence of dominant position and a loose causal connection between the conduct and the dominant position.[175] The *BkA* also noted the similarity of the balancing factors in both competition law and data protection law, one of which is dominance, and how such may led to the same outcome, which explains the statement that the balancing of interests may be done "simultaneously under competition and data protection law."[176]

Constitutional norms and principles are referred to as meta-principles that guarantee a level of consistency in terms of the interpretation between competition and data protection law as to the duties imposed dominant firms.[177] For the *Bundeskartellamt* this "unifies the balancing framework."[178]

The *BkA* did not take issue with the lack of an economic quantification of the abusive conduct in terms of comparing the net consumer harm and benefit to a counterfactual, which is often required for the analysis of other exploitative

[172] *Ibid*, [880].
[173] *Ibid*, [889].
[174] *Ibid*, [891].
[175] *Ibid*, [892].
[176] *Ibid*, [894].
[177] *Ibid*, [895].
[178] *Ibid*, [901].

practices, such as excessive pricing.[179] Such economic quantification hardly seems possible in this case. However, the lack of economic quantification cannot negate the finding of consumer harm.[180] The potential of harm is even more likely to occur in view of the perverse incentives of the data controllers to harvest "too much data," as they may benefit from the increased monetization potential of an extensive data collection, while users "bear the bulk of the potential financial (and intangible) costs incurred."[181] In any case, the *BkA* rejected any attempt by a dominant undertaking to justify restrictions of data protection, on the basis of possible positive effects that such violations may bring to its economic performance. The *BkA was arguably even more likely to reject any attempted justification of a restriction of data protection if such* concerned the fundamental rights of individuals.[182] This indicates that it is not possible for dominant undertakings to submit objective justifications for their alleged anti-competitive conduct. This arguably brings the approach followed by the *BkA* close to establishing a *per se* prohibition on dominant undertakings violating data protection rules provided there is some loose causal link between the data protection infringement and the relevant firm enjoying some degree of market power.

The *BkA*'s Facebook case constitutes one of the first examples of exploitative conduct cases involving UTCs and UCPs and their effects on privacy. The authority sought to interpret competition law and data protection law in a consistent manner and to establish a conceptual framework that would enable the simultaneous application of both areas of law. Concepts of data protection law were repurposed to match existing concepts and concerns in competition law, which has become known by some as adopting a strategy of "cross-institutional isomorphism".[183] The Facebook case is still pending on appeal at the level of the Higher Regional Court Dusseldorf, a previous preliminary decision of the Higher Regional Court Dusseldorf that ordered the suspensive effect of the appeal due to serious doubts as to the legality of the BkA's decision[184] being overruled by the German Supreme Court (BGH) in June 2020, the BGH provisionally confirming the BkA's findings.[185] Interestingly, the BGH did not find decisive, as did the BkA in its decision, the fact that

[179] *Ibid*, [906].

[180] *Ibid*, [909]. This may hint at the possibility of behavioural harm, explored in Section 3.2.5. but the Bundeskartellamt does not provide any further detail as to the way in which behavioural changes may harm users.

[181] *Ibid*, [911].

[182] *Ibid*, [913].

[183] Commenting on such a strategy, among various other options, see I. Lianos. 2018. "Polycentric Competition Law," *Current Legal Problems*, 71(1): 161, who states that this strategy involves "the borrowing of instruments and/or the overall logic from a different institutional realm and transplant them back, "repurposing them for the occasion."

[184] See, https://openjur.de/u/2179185.html .

[185] See, https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Pressemitteilungen/2020/23_06_2020_BGH_Facebook.pdf?__blob=publicationFile&v=2 .

the processing and using of personal Facebook user data was generated based on their online behaviour outside facebook.com and irrespective of whether they are logged in to Facebook and the issue of whether such an approach is compatible with the rules of the General Data Protection Regulation, but the fact that consumers were "locked in" and that the terms of service of Facebook deprived private Facebook users of any choice as to whether they wish to use the network in a more personalized way linking the user experience to Facebook's potentially unlimited access to characteristics also relating to the users' "off-Facebook" use of the internet; or as to whether they want to agree to a level of personalization, which is based on data they themselves share on facebook.com.

The need for a "catch-all" provision?: Other alternatives for privacy protection The possibility for a specific conduct to fall under another area of law that prohibits abusive contractual or trading terms is always in the background. Different jurisdictions may make different choices as to the regulatory strategy that is to be adopted. For instance, similar types of data harvesting have been sanctioned in Italy on the basis of consumer protection law.[186]

In the United States, additional possibilities are offered through specific tools, such as Section 5 of the FTC Act, which focuses on unfair and/or deceptive acts and/or practices in or affecting commerce. In the context of the assessment of the merger between Google and DoubleClick, an FTC order required Facebook to secure consumers' affirmative consent before altering their privacy settings.[187]

In 2011, Facebook settled charges with the FTC that it had deceived consumers when it had refused to keep its privacy promises. In a letter to Facebook dated 10 April 2014, the FTC stated that WhatsApp had notified its users about the limited nature of the data it collects and shares with third-parties. This letter highlighted that WhatsApp's' promises exceeded the protections enjoyed by Facebook users. The FTC wrote for the purpose of warning Facebook that it needed to continue to honour WhatsApp's promises to its users and that any breach could violate Section 5 FTC Act.[188] The FTC referred to WhatsApp's privacy policy, dated 7 July 2012, which sets out the type of the data that WhatsApp collects. The FTC noted that hundreds of millions of users chose to use WhatsApp's service based on the promises of privacy that it articulated in that notice. After announcing its decision

[186] See, https://www.agcm.it/media/dettaglio?id=1b36a40a-25b6-4056-9d34-1a07adf34a5e .

[187] FTC. 2014. "FTC Notifies Facebook, WhatsApp of Privacy Obligations in Light of Proposed Acquisition," Press Release, <https://www.ftc.gov/news-events/press-releases/2014/04/ftc-notifies-facebook-whatsapp-privacy-obligations-light-proposed>.

[188] FTC. 2014. "Letter from Jessica Rich to Facebook and WhatsApp," Letter, 1, <https://www.ftc.gov/public-statements/2014/04/letter-jessica-l-rich-director-federal-trade-commission-bureau-consumer>.

to acquire WhatsApp, both Facebook and WhatsApp publicly stated that Facebook would abide by the promises in WhatsApp's privacy policies. The FTC intimated that the statements in WhatsApp's privacy policy represented enforceable promises to consumers about the manner in which WhatsApp collected and used their data. The FTC viewed any failure to keep promises in relation to privacy as a deceptive practice under Section 5. Further, the FTC further considered this Section as being applicable when a company uses data in ways that breach, or are materially inconsistent with, legally binding promises when it collected the data, unless consumers have expressly consented to any changes. WhatsApp's privacy policy stated that it would neither use its users' information for advertising purposes nor sell that information to third parties for commercial or marketing purposes without obtaining the individual user's consent. The FTC recommended that Facebook follow that procedure and that consumers should be provided with the opportunity to opt-out of any changes. Alternatively, Facebook should notify consumers that they can stop using the WhatsApp service. Finally, the FTC referred to its 2011 Order, which prohibited Facebook from misrepresenting the way in which it maintains the privacy and/or security of consumers' personal information. It reminded Facebook that the Order requires it to obtain the express consent of consumers before sharing their non-public information in a way that "materially exceeds any privacy setting."

Issues of privacy also arose in the aftermath of the Facebook/Instagram merger. In August 2012, the FTC closed its non-public investigation of the merger between Facebook and Instagram without taking any action. This unanimous decision permitted the parties to complete the deal.[189]

A few years later, the privacy practices of Facebook came under scrutiny again.[190] Facebook users can reveal intimate information about themselves. A user's "likes" of public pages are generally considered to be an accurate indicator of that user's personality traits. Facebook had informed users that they can control the privacy of their personal information by adjusting their privacy settings and had emphasized such to encourage users to share information. Starting in 2010, each user who installed Facebook's app had consented, through the app's default settings, to Facebook sharing, with the third-party developers that had created the app, information about both the app user and the app user's Facebook Friends, even if those friends had not installed the app, that is, "affected friends." These affected friends could only opt-out of this disclosure on Facebook's applications page, located on its website. They could not opt out from Facebook's privacy settings page. Third-party app developers used that information to enhance the in-app experience and/or

[189] FTC. 2012. "FTC Closes Its Investigation into Facebook's Proposed Acquisition of Instagram Photo Sharing Program," Press Release, <https://www.ftc.gov/news-events/press-releases/2012/08/ftc-closes-its-investigation-facebooks-proposed-acquisition>.

[190] *U.S.A. v. Facebook*, Complaint for Civil Penalties, Injunction, and Other Relief, Case No. 19-cv-2184 (D.D.C. 24 July 2019).

enhance targeted advertising to app users and affected friends. They could use that information for identity theft, phishing, fraud and/or other harmful acts.

In response to a 2012 FTC investigation, Facebook settled claims that sharing the data of Affected Friends with the third-party developers of apps deceived users. The FTC issued an Order that prohibited Facebook from misrepresenting consumers' ability to control the privacy of their information, the protocol to exercise the controls and the boundaries to which Facebook adheres when making user information available to third-parties.

After that FTC investigation, Facebook retained the same policy but posted a disclaimer on its privacy settings page informing users that the information they share with Facebook Friends would be made available to the app developers. Four months after the FTC finalized the 2012 Order, Facebook removed its disclaimer whilst it continued to share the data of Affected Friends with third-party developers and used the same separate opt-out setting. At a conference in April 2014, Facebook promised that it would stop third-party developers from access data about Affected Friends. Facebook informed third-party developers that existing apps would only be able to continue to collect Affected Friend data for one year, up until April 2015. After that date, Facebook entered into arrangements with dozens of developers to enable them to continue with their collection of the data of Affected Friends. For a sub-group of app developers, that privilege lasted until June 2018.

According to the complaint, tens of millions of users relied on Facebook's privacy claims about confining the sharing of their information to Facebook Friends. Facebook knew or should have known that sharing the data of non-consenting friends with app developers violated the 2012 Order such conduct had previously been termed "deceptive" by the FTC in regard to the original Complaint that prompted the 2012 Order. The 2012 Order required Facebook to maintain a reasonable privacy programme that safeguarded the privacy, confidentiality and integrity of user information. This obligation was critical because Facebook had been conveying the private information of app users and Facebook Friends to millions of third-party app developers. Facebook neither tracked that data in an organized and systematic manner nor do it vet third-party developers before bestowing them with access to consumer data.

The complaint reasoned that Facebook did not enforce its privacy terms adequately and was, instead, influenced by the financial benefit that third-party app developers provided in return.[191] The severity of any consequences for violating its privacy terms and the speed with which they were administered depended on the (subjective) financial benefit that the developer offered to Facebook.[192] The FTC viewed this conduct as unreasonable.

In addition to but separate from the violation of the 2012 Order, the complaint decided that Facebook violated Section 5(a) FTC Act by pursuing

[191] *Ibid*, [88]-[90].
[192] *Ibid*, [123].

deceptive practices. Facebook had asked its users to give personal information to benefit from security measures on the Facebook website or mobile application, including the user's phone number.[193] This phone number would then be used as part of a two-factor authentication process. However, Facebook also, without telling its users, used these phone numbers for advertising purposes.[194]

The final act that the FTC challenged related to privacy and facial recognition technology. In April 2018, Facebook revised its data policy to inform users that it would use the latest facial-recognition technology to identify people in pictures and videos that users uploaded if the relevant user had enabled such feature. This suggested that users needed to opt in to use facial recognition. However, tens of millions of Facebook users who used older versions of social media service needed to opt-out to disable the facial-recognition technology. The contract violated the 2012 Order by misrepresenting how consumers could control the privacy of their information.[195]

Facebook ultimately agreed to pay a USD $5 billion penalty and incorporate restrictions and a modified corporate structure that the FTC had designed to bring more accountability for decisions the company made about users' privacy. Facebook must create an independent privacy committee within its board of directors. It must certify, on a quarterly basis, that it is complying with the privacy programme mandated by the Order. It must also review every new or modified product for privacy before implementing it and must document its decisions about user privacy.[196]

It should be noted that these issues may also be tackled from the perspective of data protection law. These various options should not be considered as substitutes that require the choice of one among many possible tools but as complements, to the extent that it is possible for a specific conduct to simultaneously constitute an infringement of competition law and another area of law (for example, data protection law, unfair commercial practices and so forth). Such approach may be emulated by other jurisdictions, particular in the BRICS countries.

5. *Exploitative Requirement Contracts*

A possible theory of harm may result from the requirement imposed by contracts that users provide their personal data in return for access to bundled digital services (see Section 2.1.). The relevant standard could be that employed in relation to tying arrangements, although such standard should cater for the

[193] *Ibid*, [13].
[194] *Ibid*, [142]-[143].
[195] *Ibid*, [14].
[196] FTC. 2019. "FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook," Press Release, <https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions>.

specific theory of harm resulting from the reduction of privacy standards, the manipulation and/or exploitation of consumers and the reduction of consumer surplus and/or wellbeing.

The conditions for such standard are the following. First, the undertaking in question is dominant in the tying market (the market for the "free product," such as social network services, or Internet search services). Second, the tying and tied goods are two distinct products. This is, of course, the case as the market for personal data is different to that for social network or search services. Third, the tying practice is likely to have an exploitative effect that harms the user, such as the loss of consumer surplus, wealth transfer, the reduction of innovation, the reduction of privacy, behavioural manipulation and/or loss of autonomy. Fourth, the tying practice cannot be objectively justified on the basis of efficiencies from which the users benefit, such as the data harvesting improving the quality of the service or product provided to the user (for example, personalization with its positive welfare effects). This theory of harm may be standalone or may be combined with one of the other theories of harm explored in this Section.

6. Behavioural Manipulation

The "exploitation of attention"[197] and "attention theft"[198] have been put forward as new forms of exploitative conduct in the digital age. However, the theoretical contours of these new forms of exploitation have been sketchy and little has been done in terms of converting them into operational standards for the purpose of competition law. Furthermore, it has been stressed that competition law needs to promote competitive attention markets.[199] Currently, the literature on behavioural manipulation lacks solid foundations. It does not take into account the significant psychological research conducted on manipulation or on the foundations of human consciousness. This is key to understand the crucial distinction between situations in which an individual by paying attention to something expresses its own individual autonomy, and those in which attention has been "captured" through some restriction of that same autonomy.

[197] Wu, T. *The Attention Merchants* (Atlantic Books, 2016), 23. See also on "human attention" as a scarce resource, See, Goldhaber, M. 1997. The Attention Economy and the Net. *First Monday*, 2(4), <http://www.firstmonday.org/issues/issue2_4/goldhaber/> ; Camerer, C. F., Johnson, E. J. Thinking about attention in games: Backward and Forward Induction. In Brocas, I., Carrillo, J. D. (eds.), The Psychology of Economic Decisions (vol.2.): Reasons and Choices (Oxford University Press, 2004), 111–129; Falkinger, J. March 2005. Limited Attention as the Scarce Resource in an Information-Rich Economy (IZA Discussion Paper No. 153), available at Limited Attention as the Scarce Resource in an Information-Rich Economy (iza.org).

[198] Wu, T. 2017. "The Attention Economy and the Law," *Antitrust Law Journal*, 82: 771.

[199] Newman, J. 2019. "Attention and the Law," Paper, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3423487>.

Before accepting the possibility of manipulation, there lies a more fundamental debate—the nature of human consciousness. Phenomenology and Cartesian thinking insist on there being a distinction between the brain and the mind. This perspective carefully distinguishes between an "internal" world and an "external" world. It divides our phenom in three parts.[200] First, our "experiences of the external world, such as sights, sounds, smells, slippery and scratchy feelings of head and cold, and of the positions of our limbs."[201] Second, our "experiences of the purely internal world, such as fantasy images, the inner sights and sounds of daydreaming and talking to yourself, recollections, bright ideas, and sudden hunches."[202] Third, our "experiences of emotion or 'affect'... ranging from bodily pains, tickles, and 'sensations' of hunger and thirst, through intermediate emotional storms of anger, joy, hatred, embarrassment, lust, astonishment, to the least corporal visitations for pride, anxiety, regret, ironic detachment, rue, awe, icy calm."[203] This approach distinguishes between the brain, in which these stimuli are processed, and the self, the "centre of narrative gravity," with the latter forming the "core" of a person and the foundation of their autonomy.

Research in psychology, specifically the "trait theory," has also put forward a "Five Factor Model" to describe the personality trait structure of all humans and offer some measurement of character.[204] The Five Factor model assumes that people have transcontextual personality dispositions that are highly stable over the course of time, different situations and social roles, with these traits characterizing "our very selves."[205] Hence, "to be true to oneself is to behave in consistent accordance with one's own latent traits."[206] These five personality trait factors are also universal and transcultural and are linked to the biological unity of humans.

However, other approaches emphasize the great maniability of human consciousness. According to the "Multiple Drafts" model, "all varieties of perception – indeed all varieties of thought or mental activity – are accomplished in the brain by parallel, multitrack processes of interpretation and elaboration of sensory inputs," with "information entering the nervous system"

[200] Dennett, D. *Consciousness Explained* (Back Bay Books, 1991), 45.
[201] *Ibid*, 45.
[202] *Ibid*, 45.
[203] *Ibid*, 45.
[204] Wiggins, J. *The Five-Factor Model of Personality: Theoretical Perspectives* (Guilford Press, 1996).
[205] McCrae, R., Costa, P. Jr. 1984. "Personality is Transcontextual: A Reply to Veroff, *Personality and Social Psychology Bulletin*, 10: 175–217; McCrae, R., John, O. 1992. "An Introduction to the Five-Factor Model and its Applications," *Journal of Personality*, 60: 175; McCrae, R., Costa, P. Jr. 1994. "The Stability of Personality: Observations and Evaluations," *Current Directions in Psychological Science*, 3: 173.
[206] Sheldon, K., Ryan, R., Rawsthorne, L. Ilard, B. 1997. "Trait Self and True Self: Cross-Role Variation in the Big-Five Personality Traits and Its Relations with Psychological Authenticity and Subjective Well-Being," *Journal of Personality and Social Psychology*, 73(6): 1380.

being "under continuous editorial revision."[207] Such an approach emphasizes the development of streams of content that are subject to "continual editing by many processes distributed in and around the brain, and continuing indefinitely into the future," without there being a "single narrative" (a "final" or "published" draft),[208] as understanding is a property that "emerges from lots of distributed quasi-understanding in a large system."[209] "Probing this stream at various intervals produces different effects, precipitating different narrative – and these are narratives."[210] "Any narrative . . . that does get precipitated provides a "time line," a subjective sequence of events from the point of view of an observer."[211] This theory may raise interesting questions as to the definition of that which constitutes "manipulation" and, in particular, if such concept would be appropriate in the circumstances of the "Multiple Drafts" model and the different means through which it could be exercised. However, this approach and its empirical foundations have been subject to criticism and the conclusions reached may not hold.[212]

Others have challenged the stability and the ahistorical and asocial nature of personality traits, arguing instead that these traits may have been influenced by culture or the specific social context and, thus, be culturally and historically conditioned and stem from "cohort effects."[213] Hence, they may be altered, making manipulation possible.

Organismic- and existentially-informed theories of personality advance a more "contextual and dynamic view of the person," with their central point being that "people do not always act in accord with their self; instead, they vary from situation to situation in the degree to which they contact and enact their true feelings and values."[214] Hence, to be true to oneself within a specific role is "to be able to behave in ways that feel personally expressive . . . , authentic . . . , or self-determined."[215]

[207] *Ibid*, 111.
[208] *Ibid*, 113.
[209] *Ibid*, 439.
[210] *Ibid*, 135.
[211] *Ibid*, 136.
[212] Akins, K. 1996. "Lost the Plot? Reconstructing Dennett's Multiple Drafts Theory of Consciousness," *Mind and Language*, 11(1): 1.
[213] See Cattell, R. 1943. "The Description of Personality. 1. Foundations of Trait Measurement," *Psychological Review*, 50: 559; Cattell, R. 1943. "The Description of Personality: Basic Traits Resolved into Clusters, *Journal of Abnormal and Social Psychology*, 38: 476.
[214] Sheldon, Ryan, Rawsthorne and Ilard, (205), 1380.
[215] See *ibid*; Waterman, A. 1990 "Personal Expressiveness: Philosophical and Psychological Foundations," *Journal of Mind and Behaviour*, 11: 47; Ryan, R. "Agency and Organization: Intrinsic Motivation, Autonomy and the Self in Psychological Development" in *Nebraska Symposium on Motivation: Developmental Perspectives on Motivation* (edited by Jacobs, J. Volume 40, University of Nebraska Press, 1993), 1; Deci, E., Ryan, R. *Intrinsic Motivation and Self-Determination in Human Behaviour* (Plenum Press, 1985).

Behaviour, (B), is, therefore, a function resulting from one's the personality, (P) and the environment, (E), in which one finds oneself, (B = f(P, E)[216]. Behaviourists, such as Skinner choose to focus more on the physical environment. Although Skinner rejects the existence of the self/ the mind, he was more interested in observable behaviour, as opposed to internal events like emotion. He reasoned that through "operant conditioning" an individual can make an association between a particular behaviour and a consequence.[217] The concept of reinforcement also emphasizes the fact that behaviour that is reinforced tends to be repeated and, thus, strengthened, whereas behaviour that is not reinforced tends to be extinguished and, thus, weakened. Behaviour may, therefore, be influenced by reinforcers, as well as by punishers who will decrease the likelihood of certain behaviour being repeated. According to behaviourists, it is possible to modify and shape behaviour through operant conditioning, for instance, by a system of tokens later exchanged for rewards.

Other approaches focus on internal psychological states, even non-conscious mechanisms. The "self-determination" (henceforth, "SD") theory offers a motivational account of behaviour. It assumes that individuals are active organisms acting on the basis of internal structures and, thus, make use of both their internal and external environments. Motivation relates to "energy, direction, persistence and equifinality; characterising activation and intention."[218] Hence, human motivation may be intrinsic. Human beings when performing an activity make use of internal structures, which form part of their perception of the phenomenal core of the *self*, as well as extrinsic factors, to the extent that human behaviour occurs for reasons other than the activity itself. SD theory distinguishes between "autonomous motivation" and "controlled motivation."[219] The former comprises both intrinsic motivation and the types of extrinsic motivation that people have identified with an activity's value and ideally will have integrated it into their sense of self and will, thereby, experience a "self-endorsement of their actions." Conversely, the latter "consists of both external regulation, in which one's behaviour is a function of external contingencies of reward and punishment, and introjected regulation, in which the regulation of action has been partially internalised and is energized by factors, such as an approval motive, avoidance of shame, contingent self-esteem, and ego-involvements."[220] Behaviour is energized and

[216] Lewin, K. "Behaviour and Development as a Function of the Total Situation" in *Manual of Child Psychology* (edited by L. Carmichael, Wiley, 1946), 791.

[217] See Skinner, B. *The Behaviour of Organisms: An Experimental Analysis* (Appleton-Century, 1938); Skinner, B. *Science and Human Behaviour* (Simon and Schuster, 1953).

[218] Ryan, R., Deci, E. 2000. "Self-Determination Theory and the Facilitation of Intrinsic Motivation, Social Development and Well Being," *American Psychologist*, 55(1): 69.

[219] Deci, E., Ryan, R. 2008. "Self-Determination Theory: A Macro-Theory of Human Motivation, Development and Health," *Canadian Psychology*, 49(3): 182.

[220] *Ibid*.

directed by autonomous and controlled motivation as well as the lack of motivation and intention marking the other pole, that is, amotivation[221].

Theoretical and empirical research has shown that autonomous motivation, which is located in the categories of intrinsic motivation, integrated regulation and identified regulation, "tends to yield greater psychological health and more effective performance of heuristic types of activities."[222] There is also evidence that a controlled regulatory environment depletes energy and may affect vitality and, thus, performance. Hence, options should be offered to users in a non-controlling way, if autonomy is to be preserved rather than undermined. Even if law and policy may only impact upon one only dimension of the broader environment that affects an individual's autonomy, psychological research may provide a substantial amount of wisdom when it comes to defining possible theories of user/consumer harm in competition law and, therefore, may provide some relief from corporate conduct that reduces autonomy.

Self-determination and autonomy may be reduced by corporations actively manipulating consumer biases.[223] In digital markets, the potential for manipulation to occur on an industrial scale has led to an emerging body of scholarship. It seeks to define manipulation in both offline and online contexts,[224] noting the concerns by regulators.[225] Large digital platforms can reach across the various dimensions of human experience. They are "dynamic, interactive and intrusive" and set forth "incisively personalisable choice architectures" capable of steering consumer choice.[226] The increasing accuracy of psychographic profiles and personality traits has become the new normal in the data economy. It drives business practices and has enabled advertising to be targeted at consumers on an individual level—no effective comparison can be drawn between this and traditional forms of advertising.

[221] See, Ryan, R., Deci, E. 2000. "Intrinsic and Extrinsic Motivations: Classic Definitions and New Directions," *Contemporary Educational Psychology*, 25: 54.

[222] See Deci and Ryan (225), 183; Nix, G., Ryan, R., Manly, J., Deci, E. 1999. "Revitalization Through Self-Regulation: The Effects of Autonomous and Controlled Motivation on Happiness and Vitality," *Journal of Experimental Social Psychology*, 35(3): 266; Chirkov, V., Ryan, R., Sheldon, K. "Human Autonomy" in *Cross-Cultural Context: Perspectives on the Psychology of Agency, Freedom and Well-Being* (Springer, 2011).

[223] Hanson, J., Kysar, D. 1999. "Taking Behavioralism Seriously: The Problem of Market Manipulation," *New York University Law Review*, 74: 630.

[224] See Calo, (129), 995; Posner, E. 2015. "The Law, Economics, and Psychology of Manipulation," University of Chicago Coase-Sandor Institute for Law and Economics Research Paper No. 726; Borgesius, F. *Improving Privacy Protection in the Area of Behavioural Targeting* (Kluwer Law International, 2015); Zarsky, T. 2019. *Privacy and Manipulation in the Digital Age, Theoretical Inquiries in Law*, 20: 157; Spencer, S. 2019. "The Problem of Online Manipulation," Paper, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3341653> ; Susser, D., Roessler, B., Nissenbaum, H. 2020. "Online Manipulation: Hidden Influences in a Digital World," *Georgetown Law Technology Review* 4: 1.

[225] European Data Protection Supervisor. 2018. "Online Manipulation and Personal Data," Opinion 3/2018.

[226] Susser, Roessler and Nissenbaum, (222), 2.

Calo expressed the problem of self-determination and autonomy of digital consumers as being one that is linked to the mediatory role of technology enabling some business actors "to design every aspect of the interaction with the consumer."[227] One may certainly envision manipulation as involving an intervention that changes the way an individual behaves and that but-for this intervention said individual would have behaved differently. Susser, Roessler and Nissenbaum note that intervention may take the following two forms. The intervention may change the "decision space" of an individual, for instance, by changing the options available to them.[228] It may also change "their internal decision-making process," that is, "the way in which they understand their options."[229]

The difficulty lies in determining that which distinguishes manipulation from other forms of intervention, such as simple influence and/or persuasion. The latter forms of intervention do not raise concerns with regard to self-determination and autonomy as they appeal to the person's decision-making power. This calls for a more precise definition of manipulation.

Spencer defines manipulation as "an intentional attempt to influence a subject's behaviour by exploiting a bias or vulnerability."[230] The manipulator targets the individual's capacity for self-governance by acting on the person's extrinsic motivations in a way that deprives them of authorship, "adjusting their psychological levers ... away from their ideal settings."[231] Similarly, the hidden nature of the manipulative influence ensures that the person being manipulated is unaware of this external regulation. Hence, situations of introjected regulation are excluded from being considered as manipulation. Susser, Roessler and Nissenbaum reason that "at its core, manipulation is hidden influence – the covert subversion of another person's decision-making power," which functions by "exploiting the manipulee's cognitive (or affective) weaknesses and vulnerabilities to steer their decision-making process towards the manipulator's ends."[232] These may be cognitive biases, emotions and/or desires.

These commentators consider that neither deception nor nudging constitute a necessary condition for manipulation: manipulation can occur without deception and not all nudges are manipulative.[233] However, coercion restricts the number of acceptable options from which a person may choose and, as

[227] Calo, (129), 1003–004.
[228] Susser, Roessler and Nissenbaum, (222), 11.
[229] *Ibid*.
[230] Spencer, (223), 4.
[231] Susser, Roessler and Nissenbaum, (222), 15.
[232] See Susser, Roessler and Nissenbaum, (222), 2; for a different position, C. Sunstein, *The Ethics of Influence: Government in the Age of Behavioural Science* (Cambridge University Press, 2016), 102–05.
[233] Susser, Roessler and Nissenbaum, (222).

such, constitutes a more direct intervention of external regulation of behaviour than manipulation.

Defining the various parameters of the concept of "manipulation" that affects human consciousness, which is a richer and deeper concept that the concept of "attention" that has so far preoccupied competition lawyers and economists[234], will be an important challenge to overcome for those arguing for the development of a manipulation theory of exploitation. It is also important to determine those sources that will be acceptable in relation to evidence of manipulation, as well as to design an appropriate test that draws on economics, behavioural economics and psychology to build a theory of consumer harm, including in general to the principle of "consumer sovereignty".[235] The legal test should also offer undertakings the possibility, following *prima facie* evidence of manipulation, to objectively justify their conduct, for instance in view of the positive outcomes for the average consumer of such "manipulation" or choose to reason that their conduct did not intend to significantly challenge the self-determination and autonomy of consumers in the specific context and thus could not be qualified as manipulation. Requiring some form of a wider market effect of such manipulation may also set a *de minimis* criterion to avoid over-regulation.

IV. REMEDIES

In view of the various market failures observed we are in favour of collective action to restore the conditions of a well-functioning data market. This may take several forms.

In the regime 2 presented, it is assumed that in the opt-out world there would be significant competition so that the purchaser of personal information would be forced to pay the competitive price that would reflect the full value of the personal information to the company, $y. If such competition among purchasers of personal information were not present, and, for example, Google remained a monopsonist, as was set out in regime 3, the user would not, to an appreciable extent, be better off in the opt-out world as opposed to the opt-in world. Therefore, any remedy cannot just involve changing the default from being opt-in to opt-out; rather, it has to achieve or, at least imitate, competition in the market for the sale of personal data.

A possible solution in relation to users having conditions imposed on them to which they did not provide their voluntary consent would be that the default regime be changed from opt-in to opt-out. In applying these principles to the case of social networks, one may reason that Facebook has no incentive to

[234] For an excellent analysis of "attention markets" see, M. Peitz, Economic Policy for Digital Attention Intermediaries (2020). ZEW - Centre for European Economic Research Discussion Paper No. 20-035, Available at SSRN: https://ssrn.com/abstract=3654009.

[235] Lerner, A. 1972. "The Economics and Politics of Consumer Sovereignty," *American Economic Rev* 62: 258.

make this change on its own and that, therefore, this has to be achieved by regulation. This is certainly the choice made by the EU as evidenced by its adoption of the GDPR, which established an opt-out regime. However, even if the default were changed to "opt-out", this by itself would not be an adequate response because the dominant social network may, as a result of its market dominance, limit access to their service unless the user "consents" to their data being harvested. Hence, due to the asymmetrical bargaining power between a digital platform that enjoys a dominant position as opposed to users, an opt-out regime will not in and of itself be enough.

One option may be to require that the digital platforms offer the same product but charge a fee to a user if said user neither wants their data to be harvested nor to be subjected to targeted advertising. In cases in which the data of the specific user is valuable, digital platforms could be required to provide a positive payment to these users so that they can join the relevant platform. However, this option would raise several issues.

Firstly, because of its dominant position Facebook could deny users "free" access to its services if they opt to exercise their privacy rights, or it could overcharge users or not pay them the competitive price to join the social network or buy their data. As discussed in Section 2.1, social networks of the size of Facebook have network effects and benefit from feedback loops. Strong network effects result in high market share inequality among networks with larger networks enjoying much greater levels of profitability while new networks are forced to overcome barriers to entry. Strong network effects can also enable larger network to subsidize "influential" users to subscribe to their services.

Secondly, as mentioned in Section 2.5, there is no market by which users can evaluate the full cost and benefit of their transaction with Facebook—the market is missing. Once the interaction between the user and the platform is understood a *market* interaction, society may more fully grasp the possibility that the dominant/monopsonistic position of the buyer of data may lead to inefficient exchanges, or that the monopsonistic buyer may have a lot of user-specific information and can implement sophisticated price discrimination strategies.

To remedy this, competition law enforcement, in particular conduct and structural remedies, in addition to other regulatory tools, such as privacy regulation, would need to work together to establish a market between users and the platform that could ensure the transparent collection of data and its use. Said market would also need to be able to ensure the provision of users' consent to the collection and specific uses of their data. It could also be developed to enable the user to be paid compensation for the "selling" of their data to a company.

Opt-out should also be the default. If a user opts-out, the relevant company, especially browsers and search engines, should not be able to use or sell the data the user discloses. Users may be compensated for opting-in, thereby,

allowing the relevant company to use the user's raw data as well as their "activities" and/or "connections." This default opt-out will create a *market* between the user and the relevant company, in which the user can sell their data to the digital platform. Users should have opt-out choice for other personal data, such as health data. They should also be able to easily set their browser to delete cookies and trackers at end of a session and users should be able to avoid Chrome.

This opens the possibility of compensating users for opting-in, that is, selling their data to the relevant company. Depending on the extent to which a user opts-in, they may be compensated in different amounts for allowing the company with which they directly interact to collect their data, to use their data for a specific purpose, and/or to sell their data to third-parties.

The EU takes a different perspective as pricing remains unaffected by the opt-in/opt-out decision. Nevertheless, the pricing of data should not be solely determined by the monopolist/dominant digital platform using its superior bargaining power vis-à-vis individual users. For this a counterfactual needs to be constructed and this raises the issue of determining the competitive monetary value of the data and ensuring that such is paid to the users (if positive pecuniary prices are charged), or the amount the users should be asked to pay (in terms of the value of their data or money) to access the product. In building this counterfactual, the decision-maker should take into account the situation prior to the competition law infringement (before-and-after test) and/or the situation in a comparable geographic market that is significantly more competitive than the market under examination.

Several other remedial options exist in terms of restricting the privacy-harming potential of digital platforms with market power, in particular indirectly through measures intensifying competition, better privacy protection being a by-product of that.

It might be possible to enhance inter-platform/inter-ecosystem competition by horizontally breaking-up the platforms and introducing several horizontal competitors into the market. The topic of breaking-up the big digital platforms has been subject to fierce discussion in recent years. This is not the first time that structural remedies, such as a break-up, have been considered as being appropriate competition law remedies. The two archetypical cases are the break-up of AT&T in 1981, and the attempted break-up of Microsoft in the early 2000s. However, previous break-up cases involved exclusionary conduct to rivals, rather than directly exploitative practices against consumers, such as harm to privacy. Note also that this remedy may be of relatively low effectiveness given the existence of the "winner-takes-most-competition" in markets with intense network effects. Even if new entrants do, in fact, enter the market, the resulting market structure may ultimately not be significantly different from that which it was before and competition will be *for* the market rather than *in* the market.

A vertical separation of the platform from the merchants, which would prohibit the platform from expanding into vertically related markets could also enhance intra-ecosystem competition and therefore provide some form of temporary relief. Such remedy, that is, a prohibition on market operators from being able to be both vertically integrated and compete in separate markets, would eliminate the incentive of the platform to commit an abuse. However, set in a direct exploitation case context, it could equally evolve to some form of regulation, a hybrid between utilities' regulation and data protection/privacy regulation.

Separation can take different other forms; it need not be structural and may concern a data separation policy (or data use break-up). It need not only focus on the dominant undertaking and the companies controlled by it but may also expand to a partial break up of their third-party ecosystem. Some "light-touch" separation may be achieved by policies that require digital platforms not to use personal data that has been harvested from participants to their ecosystems, unless they have the explicit consent of these members for the envisaged use. This may break the continuity between the data resources the undertaking commands as part of the economic entities it controls and the data resources that are provided to it by its third-party ecosystem.

Another policy could involve platforms ensuring that more protective to privacy personal data policies of companies that were acquired by a less privacy-prone digital platform stay, even after the acquisition, and are not replaced by the less privacy-oriented policies of the acquirer. The issues raised by the misleading information provided in the context of the acquisition of WhatsApp by Facebook, discussed in Section 3.1. offer a good example of this.

"Data separation" policies could be implemented more easily than structural break-ups and could serve to reduce the data advantage that some platforms have in view of the time people spend online and on each platform's ecosystem.[236] If one looks carefully at the time spent by users on the ecosystems of dominant digital platforms, it appears that the establishment of barriers regarding the use of data and the imposition of these on all members of the ecosystem may serve to reduce the barriers that new entrants face because of the data advantage of the digital platforms. This may be justified to the extent that this advantage was not acquired through organic growth but with the collaboration and considerable investment of third-party complementors that have invested in the specific ecosystem, contributed to its commercial success and built in this process relations of trust with their users. This approach regarding protection of privacy through data separation type remedies in ecosystems needs to be consistent with the approach followed with regard to privacy restrictions of competition in merger control. It would be inconsistent to take a more permissive approach in a merger context than

[236] Australian Competition and Consumer Commission. 2019. "Digital Platforms Inquiry," Final Report, 513.

in the context of an *ex post* competition assessment of an ecosystem, and allow mergers that affect privacy without proper competition law scrutiny. The fact that the data advantage of the digital platform emanates in the context of merger control from the acquisition of a rival that could have otherwise acted as competitive threat to the dominant position of the platform and possibly offer better privacy protection certainly calls for a less permissive approach. Hence, competition authorities should systematically scrutinize privacy restrictions that may result from digital mergers.

The *BkA* decision in Facebook imposed such data separation in the context of an abuse case as it prohibited Facebook from merging user and device-related data that it had collected by its own services, such as Instagram, WhatsApp, Masquerade and Oculus, with an individual user's Facebook account without said user's voluntary consent.[237] This interestingly also applied to data that has been collected by Facebook business tools on third-party websites (Facebook third-party ecosystem). The way in which Facebook collects data through those services was held to constitute an exploitative abuse of users as well as an exclusionary abuse of competitors, which violated Section 19, Paragraph 1 of the Act against Restraints of Competition.

Platforms may also opt for paying users for their data as we outlined in earlier sections, which could lead to the emergence of a licensing market for user data with users opting-in to sharing their data with specific platforms. This would enable users to port their data to the platforms that offer them higher levels of return and better conditions in terms of valuing their privacy. However, the exclusive licencing of personal data to a company would imply a monopsony and such would not solve the problem of competition in the personal data market.

Non-exclusive licensing could be instituted through a licensing agency that would collect the data from each user and distribute it to platforms. The user would be paid the combined sum of all the bids that the relevant companies are willing to pay but this raises the issue of what determines how much a user gets paid or pays. Assuming that similar competing networks exist, a user would prefer to sell their data to a larger network because when he/she joins there are more possibilities of interaction. The user's willingness to pay, $x, would increase with the size of the network. A dominant network would generally be able to pay users less and/or demand higher payments from users because of its market power and/or the data it has concerning the user's characteristics. One would expect that most users would pay more to subscribe to a large and dominant network but would be paid less by it than a smaller network.

Other remedial approaches will target the establishment of market institutions and tools reinforcing consumer sovereignty.

For instance, to determine that which constitutes a "fair" value, one would need to refer to the value of the data in a competitive market. However, this

[237] BKA Facebook, (97).

is not currently possible as there is no perfectly competitive market and there cannot be one because of network effects. Digital platforms may exercise their buying power, which could result in downward pricing pressure in the market for personal data being put on input suppliers, that is, the users. This would deprive the users from a portion of their revenues. Due to the buying power or monopsony from which digital platforms benefit and the existence of the requirement concerning the provision of data in return for access to digital services, competition law should protect users from being paid artificially low prices. In some jurisdictions, low pricing may be found to be unfair pricing and will, therefore, infringe abuse of dominance provisions.[238]

A possible solution would be for national competition authorities to facilitate users collectively bargaining, eventually in the form of collecting societies, with platforms in relation to the compensation they will receive in return for their personal data.[239] The value of personal data and, therefore, the price for which it may be sold to digital platforms may also increase if input limitations, enforced by a digital and/or data protection regulator as to, for example, the amount of data to be harvested, were established.

Data portability providing users with the ability to export their social graph or their search history constitutes another competition law remedy tackling the problem of the absence of a market for personal data. Data portability is the right of digital users to move, copy and/or transfer their personal data across different platforms. This right ensures the free flow of personal data and that users are not captive to a limited number of digital platforms. It also has important synergies from the perspective of competition law and its

[238] Unfairly low prices may also be a concern for the Article 102(a) TFEU. This does not concern predatory prices but situations in which a dominant buyer purchases inputs at unfairly low prices, which are determined by a comparison between the price paid and the economic value of the service provided. In Case C-298/83 *Comité des industries cinématographiques des Communautés européennes v Commission* [1985] ECR 1105, the CJEU examined an action for annulment against a decision of the Commission relating to the conduct of some French television stations, that held exclusive broadcasting rights, paying low license fees for the rights of films. The CJEU accepted that Article 102(a) TFEU could apply in these circumstances, although in this case the Commission had not found an abuse as it was impossible, in view of the variety of the films and the different criteria for assessing their value, to determine an administrable and valid yardstick for all films, since each film is different. This type of theory of harm is more difficult to implement in the US where, since the decision of the U.S. Supreme Court in *Weyerhaeuser* [549 U.S. 312 (2007)], high standards are required for a claim of predatory bidding to be successful. The Supreme Court also stipulated that the *Brooke Group* [509 U.S. 209 (1993)] predatory pricing analysis applies equally to the predatory pricing of outputs and predatory bidding for inputs. However, since this case, the US antitrust authorities and, more generally, the US antitrust community, have displayed a more open approach to such. In particular, they have shown concern for monopsony power in antitrust and merger control: J. Shively, "When Does Buyer Power Become Monopsony Pricing?," (2012) 27(1) *Antitrust*, 87; Hemphil, C., Rose, N. 2018. "Mergers that Harm Sellers," *The Yale Law Journal*, 127: 2078.

[239] The Economist, "Data Works of the World, Unite," (economist.com, 7 July 2018), <https://www.economist.com/the-world-if/2018/07/07/data-workers-of-the-world-unite>.

enforcement in a digital world in which access to personal data is crucial for the development of digital products and services, especially given the strong network effects and lock-in effects of multi-sided platforms. Data portability is also a data protection law remedy whose availability varies from jurisdiction to jurisdiction. In the EU, the GDPR specifies a number of rights to digital users, one of which is data portability.[240] This right requires all data subjects to be able to receive the personal data relating to them,[241] which they have provided to a controller, in a structured, commonly used and machine-readable format.[242] The GDPR also provides that, where technically feasible, the data subject shall have the right to have the personal data transmitted directly from one controller to another. This right, however, will not be applicable in situations in which the processing of the information is for the public interest or is done in the exercise of an official authority.

The United States has not passed any comprehensive federal legislation regarding privacy or data protection, although, it has enacted sector-specific regulation that has created various forms of data portability. In the healthcare domain, the Health Insurance Portability and Accountability Act (henceforth, the "HIPAA") gave patients a federal right to access their health records.[243] The 2010 Dodd-Frank Act created data portability rights regarding financial and account information and this extends to authorized third parties.[244] In the last relevant sector, Congress permitted consumers to access credit scoring information and receive an annual free credit report.[245]

On the state level, California has led the way with the California Consumer Privacy Act, which came into effect in January 2020. This statute providers users with the right to data portability—consumers may request personal information that both online and offline businesses must provide in a format conducive to portability.[246] In terms of scope of the data portability right, California's provision goes further than the equivalent requirement in the EU,

[240] Such as the right to be forgotten, the right to be notified of a breach, the right to access, the right to privacy by design, the right to restrict data processing, the right to object and rights in respect of decisions involving automated processing and profiling.

[241] Article 1: 'personal data' means any information relating to an identified or identifiable natural person ('data subject'). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

[242] Controllers must make the data available in a structured, commonly used, machine-readable and interoperable format that allows the individual to transfer the data to another controller: see Article 20 and Recital 68 of the GDPR – Right to Data Portability.

[243] Determann, L. 2019. "Healthy Data Protection," *UC Hastings Research Paper*, 7–8.

[244] Leonard, P. 2017. "Regulatory Trends and Emerging Practices in Access to Customer Data, Portability and Data Sharing in the Financial Services Sector," Daya Synergies Pty Limited, 16 and 28.

[245] Chandler, A., Kaminski, M., McGeveran, W. 2019. "Catalysing Privacy Law," University of Colorado Law Legal Studies Research Paper No. 19–25, 16.

[246] See Goldman, E. 2019. "An Overview of the California Consumer Privacy Act," Santa Clara University Legal Studies Research Paper, 2 and 5; de la Torre, L. 2018. "A Guide to the

in that it applies to inferred data concerning an individual whereas the GDPR exempts this sort of data.[247] Several States have proposed, or are investigating, data privacy laws and are basing such on the California model.[248]

Beyond the statutory route to data portability, U.S. consumers could pursue a common law claim premised on contractual law. A Restatement of the Law on Consumer Contracts, which is currently pending, may offer guidance to courts as to whether privacy policies should be viewed as contracts.[249] The debate as to whether privacy policies should qualify as enforceable contract rights relates to data portability because several of the leading online platforms have self-regulated and have created data portability rights that would comply with Article 20 of the GDPR.[250]

There is still room to develop national data protection and data portability regulations in the United States, but also the BRICS.[251] Except for some sectoral and state legislation, the United States lags behind the EU in this regard. In Brazil, India and China, data portability has either been adopted through legislation, provided for under draft law or has been stipulated under relevant standards, whereas in Russia and South Africa, their respective laws do not provide for this right.

Although the right to data portability was not primarily designed for the purpose of combatting monopolies and market power, it will have a significant impact on competition in digital markets. Multi-sided digital platforms are characterized by high network and lock-in effects. In an environment in which undertakings compete *for* the market rather than *in* the market, resulting in a "winner-takes-most," market structure, the right to data portability may provide some relief from the power held by large digital platforms. It is important to note that this right only covers personal data. Lock-in effects might not be solely limited to personal data. Furthermore, data portability may also have some anticompetitive effects. Indeed, some have reasoned that as the right to data portability will also be imposed on small and new competitors and their potential competitors as well, the imposition of the right to portability

California Consumer Privacy Act of 2018," 14, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3275571>.

[247] 29—Working Party Guidelines on the Right to Data Portability, (2017), 10 (2017); California Civil Code Sections 1798.140 (o), (l), (k), (m)).

[248] Chandler, A., Kaminski, M., McGeveran, W. (245), 28–34.

[249] They may just state company policy: Elvy, S.-A. 2018. "Commodifying Consumer Data in the Era of the Internet of Things," *Boston College Law Review*, 59: 442.

[250] Gans, J. 2018. "Enhancing Competition with Data and Identity Portability," The Hamilton Project (Brookings), Policy Proposal, 12, which lists Google, Facebook, Twitter and LinkedIn.

[251] For further analysis, see Chapter 5.4.2.5.3. of the BRICS Digital Era Competition Report (September 2019), available at http://bricscompetition.org/materials/news/digital-era-competition-brics-report/.

may result in competing firms designing their products in a format that is compatible with the incumbent, which could stifle innovation.[252]

Data portability is an important addition to data protection laws and with the extraterritoriality aspect of the GDPR it is becoming a standard norm internationally. It is probable that there would be some interesting cross-fertilization between the emerging case law on data protection and that on competition law regarding the various forms that a data portability remedy may take.

The constitution of a "data commons" may also facilitate the development of new entry into data-related markets and, therefore, such should be promoted. This may be done by, for instance, enabling the diffusion of data that has been harvested by government bodies, as has been the case in the EU with the Public Sector Information Directive[253] and, more recently, the Open Data Directive, under strict privacy-protective norms.[254] Another option would be to promote the development of "data clubs" that operate on an open, non-exclusive basis and different companies to pool and share data, again respecting high privacy standards, although, such would have to be properly scrutinized to prevent them from serving as facilitators for cartel activity limiting the protection of privacy.

Problems arise in situations in which one undertaking has a data bottleneck and, therefore, becomes a crucial node of the value chain in regard to the diffusion of information and the realization of the productive process. This includes situations in which undertakings hold an essential facility. In this context, NCAs (and/or sector specific regulators) that conclude that an infringement of competition law has occurred may impose "interoperability" as a remedy. Interoperability remedies may help to intensify inter-platform competition, thus also contributing to a better protection of privacy-related competition. For instance, Facebook could change from a closed to an open communication network by adopting open API for user messages, chats, posts and other communications. This would enable its users to send messages to users of other social networks. This could unlock privacy-related competition between Facebook and other social media, by eroding the number and identity of users' barrier to entry of Facebook that may lock in users that also value privacy but have no alternative competitive platform to switch to while keeping the possibility to communicate with their existing social network.

Finally, it is important to add the existence of technological solutions to the problem of restrictions to privacy by the business conduct of digital platforms or, more generally, user-initiated and driven practices that may frustrate the

[252] Cowen, T. "Marginal Revolution," (marginalrevolution.com, 18 May 2018), <https://marginalrevolution.com/marginalrevolution/2018/05/forced-data-portability-mistake.html>.

[253] Directive 2013/37/UE amending Directive 2003/98/EC on the Re-Use of Public Sector Information, [2013] OJ L 175/1.

[254] Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on Open Data and the Re-Use of Public Sector Information, [2019] OJ L 172/56.

aims of the advertisement-based business models, such as Adblocks[255] and the development of tracking protection technologies.[256] For instance, national competition authorities may require the development of a unique "do-not-track" switch that could apply to all networks and prohibit or even highlight exploitative abuse of dominance cases against companies if they try to bypass these technologies or forbid their use in their platforms.[257]

V. CONCLUSIONS

We have shown that the acquisition of private information by default without compensation by digital platforms such as Google and Facebook creates a market failure and can be grounds for antitrust enforcement. To avoid the market failure, the default in the collection of personal information has to be changed by law to "opt-out." This would allow the creation of a vibrant market for the sale of users' personal information to digital platforms. Assuming that all parties are perfectly informed, users are better off in this functioning market and digital platforms are worse off compared with the default opt-in. However, just switching to a default opt-in will not restore competition to the "but" for world because of the immense market power and bargaining power towards an individual user that digital platforms have acquired. Digital platforms can use this power to reduce the compensation that a user would receive for his/her personal information compared with a competitive world. Additionally, it is likely that the digital platforms are much better informed than the user in this market, and can use this information to disadvantage users in the market for personal information.

Such market failures may be dealt with by the enforcement of competition law, *ex ante* and/or *ex post*. One should be careful to distinguish this option from the possibility to implement data protection legislation, if this is available in the specific jurisdiction. The criterion of legality put forward by such legislation, the structure of its enforcement and the types of harm that may give rise to its implementation, regarding exploitative conduct that is likely to reduce

[255] Treharne-Jones, E. "The Privacy Consequences in the Rise of Ad Blockers," (iapp.org, 30 September 2015), <https://iapp.org/news/a/the-privacy-consequences-in-the-rise-of-ad-blockers/.

[256] See Camp, D. "Firefox Now Available with Enhanced Tracking Protection by Default Plus Updates to Facebook Container, Firefox Monitor and Lockwise," (blog.mozilla.org, 4 June 2019), <https://blog.mozilla.org/blog/2019/06/04/firefox-now-available-with-enhanced-tracking-protection-by-default/> ; Nield, D., "It's Time to Switch to a Privacy Browser," (wired.com, 16 June 2019), <https://www.wired.com/story/privacy-browsers-duckduckgo-ghostery-brave/.

[257] This may be necessary in view of the strategies of some of these platforms to put an end to the use of ad blocking software, see J. Aten, "Google is Putting an End to Ad-Blocking in Chrome: Here Are the 5 Best Browser Alternatives," (inc.com), <https://www.inc.com/jason-aten/google-is-putting-an-end-to-ad-blocking-in-chrome-here-are-5-best-browser-alternatives.html>.

privacy, are different from those of competition law and in no case exhaust the issues raised. Hence, in most cases it would be important to combine different regulatory fields to tackle the full dimension of the social harms of such conduct. One of the authors referred elsewhere to the need of a "toolkit approach" emphasizing the complexity of the regulatory strategy to be followed.[258] A comparison between the different set of rules applying for the assessment of mergers and that of other forms of conduct shows that there are two gap in the current system of EU competition law enforcement regarding exploitative practices reducing privacy. First, the European Commission has not so far seriously assessed the privacy effects of mergers, although it has accepted that privacy, in some cases, constitutes an important parameter of competition. However, this statement is meaningless if it is not followed by a systematic assessment of the likely exploitative effects of the merger regarding privacy. As data protection regulation does not cover all the market failures identified, and data protection regulators are not involved in the merger approval process, there is a significant gap in the protection of EU consumers and citizens.

Second, assuming that the Commission will change stance in the future, another regulatory gap emerges. If mergers are assessed also for their exploitative effects regarding privacy, the threshold of EU intervention *ex ante* will be set at the lower level than dominance, that of the existence of a significant impediment to effective competition. However, the intervention threshold for *ex post* control would be that of dominance on a relevant market. This ignores the possibility that privacy reduction practices and exploitation may find its source in conglomerate effects in the context of an ecosystem of paramount importance whose gatekeeper does not however enjoy a dominant position on a relevant market and hence elude the scope of application of Article 102 TFEU. Some national competition law regimes made some effort to deal with this gap by having recourse to their legislation regarding abuse of economic dependence,[259] or by adopting bespoke legislation, although this has so far

[258] See, Lianos, I. Competition Law for the Digital Era: A Complex Systems' Perspective (30 August 2019). Available at SSRN: https://ssrn.com/abstract=3492730 or http://dx.doi.org/10.2139/ssrn.3492730 , 160 et seq.

[259] For instance, in the Belgian law for competition which was presented recently and through which the introduction of the abuse of a relationship of financial dependency is proposed, the Belgian legislator made specific reference to digital platforms and the legislative gap, which exists as reasons for the introduction of these new laws: Loi modifiant le Code de droit économique en ce qui concerne les abus de dépendance économique, les clauses abusives et les pratiques du marché déloyales entre entreprises, Art. 4, http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=2019040453&table_name=loi; In France, the Autorité de la Concurrence has applied the provisions for the abuse of economic dependency (Article L. 420 2, alinéa 2 du code de commerce) to undertakings which do not have a dominant position in a relevant market: Case 20-D-04 16 March 2020 «relative à des pratiques mises en œuvre dans le secteur de la distribution de produits de marque Apple», https://www.autoritedelaconcurrence.fr/sites/default/files/integral_texts/2020-06/20d04.pdf . In Germany, new Article 19A in the suggested tenth amendment of the German Competition Act expands the scope of German

focused only on exclusionary behaviour[260] and does not fully integrate in competition law thinking the reality of digital "ecosystems."[261] This remains an important gap in the current design of competition law, not only in the EU, but also more broadly, and needs to be addressed.

competition law to certain specific types of conduct by an undertaking having a paramount significance for competition across markets: New Article 19a GWB-E (Referen-tenentwurf eines Zehnten Gesetzes zur Änderung des Gesetzes gegen Wettbewerbsbeschränkungen).

[260] With the exception of Article 19a2(5) GWB-E, all other examples of conduct in the suggested new provision of the German Competition Act relate to exclusionary practices. Furthermore, Art. 19a2(5) only refers to a B2B context, and does not seem to envisage its application in a B2C context. The abuse of economic dependence provisions have also always apply in a B2B context.

[261] Unless one takes the view that ecosystems may be defined as relevant markets: see, for instance, the suggestion on how to define aftermarket ecosystem markets "[…] even if in some consumer-facing markets—according to their own account—firms compete to draw consumers into more or less comprehensive ecosystems, markets for specific products or services will persist from a consumer's perspective, and should continue to be analysed separately, alongside competition on (possible) markets for digital ecosystems. Where the firms' lock-in strategies are successful, and consumers find it difficult to leave a digital ecosystem, ecosystem-specific aftermarkets may need to be defined": Crémer, J. et al. 2019. Competition Policy for the Digital Era, available at https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf . However, focusing on aftermarkets, covers only a dimension of the issues raised by ecosystem competition. The definition of power/dominant position in an ecosystem should also rely on a different methodology and metrics than defining a dominant position in a relevant market. Indeed, the current metrics and methodologies applying for the latter result from past case law and decisional practice which do not engage with issues of centrality and positional power, that are nevertheless the key factors to consider to determine power in the context of an ecosystem. See, M. Jacobides & I. Lianos, Ecosystems and competition law: From theory to practice, forthcoming Industrial and Corporate Change (2020), available at Ecosystems and competition law in theory and practice by Jacobides, M. G., Lianos, I.: SSRN.