UCL FACULTY OF LAWS

UCL

Centre for Law, Economics and Society

Research Paper Series: 5/2019

Restrictions on Privacy and Exploitation in the Digital Economy: a Competition Law Perspective

Nick Economides and Ioannis Lianos

Centre for Law, Economics and Society

CLES
Faculty of Laws, UCL

Director: Dr. Deni Mantzari

Founding Director: Professor Ioannis Lianos

CLES Research Paper Series
5/2019

Restrictions on Privacy and Exploitation in the Digital Economy: A Competition Law Perspective

Nick Economides and Ioannis Lianos

August 2019

Centre for Law, Economics and Society (CLES)
Faculty of Laws, UCL London,
WC1H 0EG

The CLES Research Paper Series can be found at https://www.ucl.ac.uk/cles/research-papers

Pre-published version of Nick Economides & Ioannis Lianos, Restrictions on Privacy and Exploitation in the Digital Economy: A Competition Law Perspective, in I.Lianos & A. Ivanov (ed.), *BRICS Digital Competition Law Report* (BRICS Competition Law and Policy Centre, 2019).

Also available as a BRICS Competition Law and Policy Centre research paper.

ISBN 978-1-910801-29-1

2019
Centre for Law, Economics and Society
Faculty of Laws, UCL
London, WC1H 0EG
United Kingdom

Restrictions on Privacy and Exploitation in the Digital Economy: A Competition Law 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 this 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 to 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. This emphasis on exploitation does not mean that restrictions on privacy may not result from exclusionary practices. However, we analyse these in a separate study. Eliminating the requirement and the market failure by creating a functioning market for the sale of personal information is imperative.

Besides the traditional analysis of the requirement and market failure, we note that there are typically informational asymmetries between the data controller and the data subject. The latter may not be aware that his data was harvested, in the first place, or that the data will be processed by the data controller for a different purpose, or shared and sold to third parties. The exploitation of personal data may also result from economic coercion, on the basis of resource-dependence or lock-in of the user, the latter having no other choice, in order to enjoy the consumption of a specific service provided by the data controller or its ecosystem, than to consent to the harvesting and use of his data. A behavioural approach would also emphasise the possible internalities (demand-side market failures) coming out of the bounded rationality,

[*] Nick Economides is professor of economics at NYU Stern Business School and executive director of the Networks Institute. Ioannis Lianos is professor of Global competition law and policy at UCL Faculty of Laws, Director of the Centre for Law, Economics and Society at UCL and Academic Director of the BRICS Competition Law and Policy Institute at the Higher School of Economics – National Research University. The authors would like to thank Tobias Kleinschmitt, Gautam Natarajan and Matthew J. Strader for their valuable research assistance. Any errors or omissions are the authors' alone. The paper expresses personal opinions and does not represent the views of the Hellenic Competition Commission.

or the fact that people do not internalise all consequences of their actions and face limits in their cognitive capacities.

The paper also addresses the way competition law could engage with exploitative conduct leading to privacy harm, both for ex ante and ex post enforcement.

With regard to ex ante enforcement, the paper explores how privacy concerns may be integrated in merger control as part of the definition of product quality, the harm in question being merely exploitative (the possibility the data aggregation provides to the merged entity to exploit (personal) data in ways that harm directly consumers), rather than exclusionary (harming consumers by enabling the merged entity to marginalise a rival with better privacy policies), which is examined in a separate paper.

With regard to ex post enforcement, the paper explores different theories of harm that may give rise to competition law concerns and suggest specific tests for their assessment. In particular, we analyse old and new exploitative theories of harm relating to excessive data extraction, personalised pricing, unfair commercial practices and trading conditions, exploitative requirement contracts, behavioural manipulation.

We are in favour of collective action to restore the conditions of a well-functioning data market and the report makes a number of policy recommendations.

***Keywords**:* digital, privacy, restrictions of competition, exploitation, market failure, hold up, merger, abuse of a dominant position, unfair commercial practices, excessive data extraction, self-determination, behavioural manipulation, remedies, portability, opt out.

JEL: K21, L12, L4, L41

Restrictions on Privacy and Exploitation in the Digital Economy: A Competition Law Perspective

Nicholas Economides & Ioannis Lianos[*]

1. Introduction

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. The concept of 'big data' is usually employed to refer to gigantic digital datasets, which are often held by corporations, governments and other large

[*] Nick Economides is professor of economics at NYU Stern Business School and executive director of the Networks Institute. Ioannis Lianos is professor of global competition law and policy at UCL Faculty of Laws, Director of the Centre for Law, Economics and Society at UCL and Academic Director of the BRICS Competition Law and Policy Institute at the Higher School of Economics – National Research University. The authors would like to thank Tobias Kleinschmitt, Gautam Natarajan and Matthew J. Strader for their valuable research assistance. Any errors or omissions are the authors' alone. The paper expresses personal opinions and does not represent the views of the Hellenic Competition Commission.

organisations, and which are 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 the tracking of webpages visitors exist since the early days of the Internet, with the rise of social media and Web 2.0, it is technologically possible for third-party websites to be embedded into the visited website through references to external resources to the website, such as a JavaScript code, which the user's browser will automatically load from the third-party server, and execute[3]

Data can be harvested by digital platforms across different devices such as smartphones, tablets and laptops/computers, for instance with regard to websites the user has interacted with (first data aggregator), or from other entities, through third party tracking, the tracker harvesting data not directly from the user, but 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 being found on more than 60% of all page loads, and Facebook 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 GDPR, has led to a decrease of the usage of third-party cookies and third-party domains.[5] Tracking capabilities are also concentrated in a few number of companies, with Google holding most power, in terms of reach of a tracker on popular websites and apps, in both websites and apps, followed by Twitter, Facebook and Microsoft for websites trackers, and Amazon, Facebook and Comscore for mobiles trackers.[6] The recent consolidation of the tracking analytics industry with the mergers of Microsoft/Linkedin (2016), Adobe/Lyvefire (2016), Facebook/Liverail (2014), Alibaba/Umeng (2013), Google/Doubleclick (2007), has also contributed to the emergence of

[1] 'Aspects of 'big data' that are often mentioned are large amounts of different types of data, produced at high speed from multiple sources, whose handling and analysis require new and more powerful processors and algorithms': Autorité de la Concurrence & Bundeskartellamt, Competition Law and Data (May 16, 2016), 4 . 'Big data' is often characterized https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election 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 adding Veracity and Validation.

[2] See, the recent controversy concerning the use of Facebook generated data from Cambridge Analytica, a political strategy firm, for uses for which Facebook's clients had not provided their consent, in particular in order to design 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, in order to target them with personalised political advertisements and influence their votes. See, https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election ; https://www.politico.eu/article/cambridge-analytica-chris-wylie-brexit-trump-britain-data-protection-privacy-facebook/ .

[3] S. Schelter & J. Kunegis, Tracking the Trackers: A Large-Scale Analysis of Embedded Web Trackers, Proceedings of the Tenth International AAAI Conference on Web and Social Media (ICWSM 2016), available at file://ad.ucl.ac.uk/homea/uctlioa/Documents/EPANT/13024-57897-1-PB.pdf .

[4] See, https://www.ghostery.com/study/ .

[5] P. Wagner, News Pages Are Abandoning Third-Party Ad Trackers, available at https://www.statista.com/chart/15578/change-of-ad-tracking-techniques-since-gdpr/ (September 25th, 2018) (noting that in Europe third party cookies decreased by 22 percent per page while third-party domains decreased by 4 percent since the GDPR became enforceable).

[6] See, R. Binns, J. ZhaoM. Van Kleek, N. Shadbolt, Measuring third party tracker power across web and mobile, (March 2010) ACM Comput. Entertain. 9, 4, Article 39, https://doi.org/0000001.0000001, available at https://arxiv.org/pdf/1802.02507.pdf (proposing a new metric for power to measure the effect of the consolidation among tracker companies).

a market structure dominated by a small number of firms, and a long tail of less significant trackers.[7]

Furthermore, data (or information) intermediaries (brokers), such as Axciom and Equifax, package information from various sources to profile customer groups. This profiling has historically aided targeted advertising. Advertisers are building campaigns based on geographies, socioeconomic factors, age, government data, same-store sales, etc. The internet spawned new variants of data brokers. Traditional intermediaries collect outcomes data on several dimensions, such as same store sales and credit history. Marrying raw purchasing history (harvested by traditional intermediaries) with ideation (with prediction platforms such as Facebook/Google) may easily build a digital customer journey. Basic statistical models would be able to determine *when* to advertise to individuals to maximize conversions. In this way, payments become far more important for future advertising revenue. Statistical models could separate window shoppers and day dreamers from serious shoppers. While this discourse focuses largely on payments, it extends to other decisions made by consumers.

Recent technological progress in data analytics may also greatly facilitate the prediction of personality traits and attributes from even a few digital records of human behaviour, such as 'likes' or facial images on Facebook,[8] while inferring identities, such as social security numbers, from anonymised data has been possible for some time.[9] The development of smart cities (with extensive networks of sensors) and technologies such as artificial neural networks enable better predictions of both actions as well as behaviours of smart cities' users, or even the formation of new social ties, through better modelling and simulation.[10] Digital technology facilitates the elaboration of advanced (even real-time) sociometrics and new applications, such as social credit experiments.

The concept of 'privacy' may be defined broadly or narrowly, and its precise contours constitute a matter of academic (and non-academic) discussion[11]. 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 personal data protection and the role competition law may play in this context.

---

[7] *Ibid*.; M. Falahrastegar, H. Haddadi, S. Uhlig & R. Mortier, Anatomy of the Third-Party Web Tracking Ecosystem (2014) arXiv:1409.1066, available at https://arxiv.org/abs/1409.1066 .

[8] M. Kosinski, D. Stillwell, T. Graepel, Private traits and attributes are predictable from digital records of human behaviour, (2013) 110 (15) Proc. Natl. Acad. Sci. U.S.A. 5802–5805.

[9] A. Acquisti, & R. Gross, Predicting social security numbers from public data, (2009) 106 (27) Proc. Natl. Acad. Sci. U.S.A. 10975.

[10] See, M. Batty, K.W. Axhausen, F. Giannotti, A. Pozdnoukhov, A. Bazzani, Smart cities of the future, (2012) 214 The European Physical Journal 481; A. Almeida & G. Azkune, Predicting Human Behaviour with Recurrent Neural Networks, (2018) 8(2) Applies Sciences 305.

[11] See, for instance, D. Solove, The meaning and value of privacy, in B. Roessler & D. Mokrosinska (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.

The EU, as well as its Member States, constitute some of the most active jurisdictions in this context, to the extent that they recognise a fundamental right to privacy[12] and they have established an elaborate system of data protection, most recently with the implementation of the General Data Protection Regulation (GDPR) and related legislation.[13] The fundamental principle of the GDPR is the requirement to have a 'legal basis' for all processing of personal data (although this does not cover 'anonymous' data)[14], six legitimate grounds being mentioned, including the requirement of explicit consent by the data subject. The GDPR obligations apply to 'controllers' which can be natural or legal persons, irrespective of whether their activity is for profit or not, irrespective of their size and whether they are private law or public law entities. Among the rights conferred to data subjects is the right to data portability, individuals having the right to receive free of charge their personal data which they provided themselves on the basis of contract or consent in a 'structured, commonly used, and machine-readable format' and to transmit the data to another controller.

In the US, the California Consumer Privacy Act (CCPA) 2018[15], and a number of sector specific data and privacy protection regimes, have been enacted at both the federal and state levels. The CCPA has similarities with the GDPR, but a more limited scope. It applies only to for profit organizations (businesses) having an annual gross revenue in excess of $25 million and doing business in California (although a business established outside of California may also fall within the personal scope of application if it collects or sells California consumers personal information while conducting business in California). It also excludes from its scope the processing of some categories of personal information (e.g. medical information and protected health information). 'Aggregate consumer information' also does not benefit from protection. In contrast to the GDPR, the CCPA does not require a 'legal basis' for all processing of personal data, nor the establishment of accountability requirements, such as the appointment of Data Protection Officers, as required by the GDPR. The right to opt-out is only available in the case of selling or sharing personal information, and does not apply to the harvesting of personal information, as it is the case in the EU, which covers all 'processing' of information. The CCPA does not include a list of grounds that businesses must adhere to a priori but relies on *a posteriori* mechanism, allowing consumers to opt-out to the sale and disclosure of their

[12] Article 7 of the Charter of Fundamental Rights lays down the right to respect for private and family life, home and communications, protecting the individual primarily against interference by the state.

[13] Article 8 of the Charter of Fundamental Rights recognises the protection of personal data as a separate right, which goes beyond simply protecting against interference by the state, but entitles the individual to expect that his or her information will only to be processed, by anyone, if however this processing is fair and lawful and for specified purposes, that it is transparent to the individual who is entitled to access and rectification of his/her information. The rights must also be subject to control by an independent authority. Article 16 TFEU requires rules to be laid down relating to data protection and to the free movement of such data in the internal market. The EU has adopted General Data Protection Regulation (EU) 2016/679 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, which applies from 25 May 2018. Its scope is significant and wide-ranging. For a commentary, see O. Lysnkey, The 'Europeanisation' of Data Protection Law, (2017) 17 Cambridge Yearbook of European Legal Studies 252. See also, Directive 2009/136/EC of 25 November 2009 (Cookie Directive) [2009] OJ L337/11; Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (ePrivacy Directive) [2002] OJ L201/37.

[14] Recital 26 of the GDPR defines anonymous information, as '…information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable'.

[15] See https://www.caprivacy.org/ .

personal information or to request the erasure of the information. If the consumer opts out, then an explicit permission is required for the sale and disclosure of this personal information. The right to data portability is also recognized as forming part of the right to access of the consumer to her data free of charge but only applies to data collected in the previous 12 months.

Similarly, privacy and data protection provisions exist in several BRICS jurisdictions.[16] In Brazil, the recently enacted in August 2018 General Data Protection Law (Law n. 13.709/2018) is inspired by the European regulatory framework, may be applied extraterritorially, and relies on consent of the individual.[17] In Russia, the Law On Personal Data provides the normative basis for the process of personal data collecting, storing and processing, again on the basis of the principle of consent by the data subject.[18] In contrast to the GDPR and the CCPA, it does not include however the right to data portability. In India, the Supreme Court declared in *Justice KS Puttaswamy And Another Vs. Union of India and Ors*, the 'right to privacy' to be part of the fundamental 'right to life' under Article 21 of the Constitution of India[19] and a draft Personal Data Protection Bill (PDPB) was suggested by the government in July 2018, and is still in consideration. It relies on the concept of explicit consent of the data subject and aims to protect the autonomy of individuals in relation with their personal data. The Bill includes a right to data portability.

The situation is different in China where, in the absence of a regime of data protection and a right to privacy, legal practice tends to apply *The Law against Unfair Competition* to provide ultimate protection when no protection can be sought elsewhere. In China, data protection mostly refers to data security and does not encompass privacy concerns. One may nevertheless observe the gradual emergence of other paths for the protection, in particular a property rights protection for data. Digital property rights holders may protect their property rights and interests in accordance with the provisions of the *Property Law*, the *Intellectual Property Law*, the *Law against Unfair Competition*, the *Tort Liability Law*, etc. depending on the nature of their different properties. However, no consensus has been reached yet on the legal nature of digital assets in China, such as industrial data and personal information.[20] In South Africa, the right to privacy is protected by the common law and section 14 of the Constitution. Personal data protection is further provided by the Protection of Personal Information Act, No 4 of 2013 (POPIA), although it is not yet in effect. As the GDRR it applies to the processing of personal data and prescribes eight specific principles for the lawful processing and use of personal information. In particular, any transferring of personal information across borders without any legal basis, including the prior consent of the party whose personal information was processed.

In addition to this emerging field of data protection, in recent years, the digital sector has attracted the attention of some competition authorities and regulators involved in data protection, which advanced the need for a more connected approach between these two areas of law, aiming to avoid the exploitation of the personal data of consumers and restrictions to

[16] For a more detailed discussion, see the relevant country reports.
[17] Law n. 13.709/2018, known in Portuguese as *Lei Geral de Proteção de Dados* – "LGPD."
[18] The Federal Law 'On Personal Data' dated 7 July 2006 No. 152-FZ <http://pravo.gov.ru/proxy/ips/?docbody=&nd=102108261> accessed 28 February 2019.
[19] https://www.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf
[20] For more detailed analysis, see the description in the country report on China in Part 4.

their privacy,[21] although the theoretical underpinnings may be different. Indeed, data protection and privacy regulations often take a fundamental rights perspective, seeing privacy as an issue of rights. Both the GDPR and its predecessor were inspired by a fundamental rights based approach as data protection and the right to privacy are protected by the Charter of Fundamental Rights of the EU - Articles 7 and 8. A distinction is also made between privacy, which is formally protected and cannot be traded, and data which can be traded following consent by the data subject. However, no existing data protection regulation establishes a property right on personal data, and confers that to the data subjects. Although the GDPR seems to be inspired by some property-like rights logic when it introduces the principles of data portability and the right to be forgotten, it stops short from recognizing property rights on data.[22] 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 the users detaining any property right on their data. A property right would involve the use as well as the possibility to sell data and license it to someone for profit, or use the data as security/collateral for raising capital, as it is the case with intellectual property rights. Although data could be considered as an intangible asset which could, in theory, be protected by property rights, this is not presently possible with personal data and there is a quite polarised discussion on this issue.[23] We do not take position as to the normative question of establishing, or not, property rights on personal data, but we analyse this to the extent that the absence of property rights may give rise to a market failure. In any case, and notwithstanding the normative question of establishing property rights on personal data, the exploitation of personal data certainly creates value, however this is entirely, or overwhelmingly, captured by the entities (e.g. digital platforms) harvesting this data, which may benefit from a monopsony and/or monopoly (market) power, this raising competition law issues, which is the main focus of this paper.

Competition law usually takes a market failure approach, and is concerned by the fact that consumer or total welfare, or well-being, may suffer from reduced data protection in a malfunctioning market for personal data acquisition, to a similar extent that it could suffer from higher prices or lower quality. In addition,, to fit better with the welfarist foundations of the economic approach in competition law, although one may also envisage the possibility of a rights-based framework,[24] a market failure approach may provide common intellectual foundations for the assessment of harms associated to the exploitation of personal data, even when the specific legal system does not formally recognize a fundamental right to privacy. It

[21] 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 (May 16, 2016); US FTC, Big Data – a Tool for Inclusion or Exclusion? (January 2016) and the references included.

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

[23] See, for instance, the discussion in P. Samuelson, Privacy as Intellectual Property, (2000) 52(5) Stanford Law Review 1125 (criticizing a property rights approach); L. Lessig, Privacy as Property, (2002) 69 *Social Research* 1; P. M. Schwartz, Property, Privacy, and Personal Data, (2004) 117 Harv. L. Rev. 2055;). N. Purtova, Do property rights in personal data make sense after the Big Data turn? Individual control and transparency, (2017) 10(2) Journal of Law and Economic Regulation 64.

[24] For a discussion, see, with regard to the right to food, I. Lianos & A. Darr, Hunger Games: Connecting the Right to Food and Competition Law (June 1, 2019). Available at SSRN: https://ssrn.com/abstract=3414032 or http://dx.doi.org/10.2139/ssrn.3414032.

may also provide the possibility of a more unified approach on theories of harm for both competition law and data/privacy protection.

For these reasons, we argue for a market failure approach, although we also recognize that there is value in protecting personal data and privacy from a fundamental rights' perspective and in any case that the two approaches are not mutually exclusive but may, and have already been, combined in order to provide the highest levels of protection.

We present a model of market failure based on a requirement provision in the acquisition of personal information from users of other products/services of Google and Facebook. 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.

Besides the traditional analysis of the requirement and market failure, we note that there are typically informational asymmetries between the data controller and the data subject. The latter may not be aware that his data was harvested, in the first place, or that the data will be processed by the data controller for a different purpose, or shared and sold to third parties. Maybe there was no consent for such use, or, if there was consent, it may not have extended to third parties' use. The exploitation of personal data may also result from economic coercion, on the basis of resource-dependence or lock-in of the user, the latter having no other choice, in order to enjoy the consumption of a specific service provided by the data controller or its ecosystem, than to consent to the harvesting and use of his data. A behavioural approach would also emphasise the possible internalities (demand-side market failures) coming out of the bounded rationality, or the fact that people do not internalise all consequences of their actions and face limits in their cognitive capacities. Hence, a user may consent on the harvesting and use of his data, without necessarily realising the full consequences and costs of his choice. This may occur in the context of an exchange in which the user is offered a free product in exchange of his data.

Dan Ariely advances the concept of 'zero-price effect', suggesting that people associate free products with pleasure, when making decisions under System 1 (intuitive decisions).[25] Some recent neuro-economics research also links payment for a product with pain, arguing for instance that consumers may react differently to the 'pain of paying' and that credit cards 'anesthetize' the pain of paying.[26] This research illustrates how decisions over providing access to personal information may be welfare or well-being reducing for individuals and that the requirement of consent, as it is set in data protection law, may not necessarily fully preserve their interests.

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 harm may result even from conduct that, at first sight, could appear as

[25] K. Shampanier, N. Mazar, & D. Ariely, Zero as a special price: The true value of free products, (2007) 26 Marketing Science**,** 742; D. Ariely, *Predictably Irrational: The hidden forces that shape our decision* (HarperCollins, 2008), Chapter 3.

[26] See, S. Rick, C.Y. Cryder, G. Loewenstein, Tightwads and Spendthrifts, (2008) 34 Journal of Consumer Research 767 (suggesting a "spendthrift-tightwad" scale, to measure individual differences in the pain of paying); S. Rick, The Pain of Paying and Tightwaddism: New Insights and Open Questions, in S.D. Preston, M. L. Kringelbach, and B. Knutson (eds.), *The Interdisciplinary Science of Consumption* (MIT Press, 2014), 147.

increasing consumer surplus. For instance, advertised-based platforms, such as Google and Facebook provide free search in exchange for acquisition of private user information. Not only these companies benefit from market power, to the extent that they control the most popular search engine and social media platforms, but also their users are locked-in since they face costs of switching to rival products. 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. 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.' The paper first engages with the different types of market failure, before addressing the way competition law has dealt and could engage with exploitative and exclusionary conduct leading to privacy harm. The final part provides some thoughts on possible remedial action, also beyond the strict confines of competition law. The paper does not engage with other forms of user harm that may result from anticompetitive conduct by platforms, such as deterioration of the quality of search query results,[27] or excessive prices extracted from advertisers in view of exclusionary practices, which are addressed in a separate paper.

2. 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. Besides the traditional analysis of market failure, we 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 the privacy and data of the 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 can provide a good complement to data protection law in this context.

[27] See, I. Lianos & E. Motchenkova, Market Dominance and Search Quality in the Search Engine Market, (2013) 9 Journal of Competition Law and Economics 419.

2.1. Market failures through exclusionary and exploitative requirement contracts bundling digital services with personal data

The antitrust concerns for advertising-based platforms, such Google and Facebook, are similar. Both companies allow free access to their respective service in return for the user granting free access to his/her personal information. This information includes IP address, cookies, location, search history and possibly parsing of emails for Google and user posting and user "likes" history for Facebook. Data collection by the companies occurs with "no questions asked" since the default is to "opt-in" in the collection processes of both companies. The default opt-in and the zero price in data collection constitute a *market failure*. That is, the market between the user and company on acquisition of personal data does not function properly as a market, and everyone participating in Google Internet search or Facebook service is giving their personal data for free. If the default were opt-out rather than opt-in and the market for data acquisition was properly functioning, users would receive various amounts of monetary compensation from the companies depending on each user's features.

Google offers free Internet search and effectively requires data provision by the user at zero price. That is, it offers Internet search *only if* the user provides data. This setup is restrictive to consumers especially those who might be willing to pay for Google service but would prefer not to share their personal information with the companies.

Imposing the requirement of personal data provision to receive Internet search increases Google's market power in the data market. A user who would not have freely given his/her personal data to Google is now doing so because this is a requirement to access Google's Internet search. Thus, this requirement increases Google's market share in the data market. Since such data is used to sell ads, Google's requirement directly increases its market power in the ads market, and stifles competition in this market. This claim is uncontroversial. As a recent ACCC shows, Google and Facebook possess substantial market power in several markets, including in online search, online advertising and news media referral as 'gateways' to online publishing.[28]

To the extent that users receiving free search do not receive in kind the full compensation for the data they provide, they are harmed by the requirement practice. Additionally, there are users who would prefer to pay for search and not to provide their personal data to Google. They are also harmed by being compelled to provide personal data under Google's requirement.

Similarly, Facebook provides free access to its service and requires data provision at zero price. It offers Facebook service only if the user provides access to personal data. Imposing the requirement of data provision to receive Facebook service increases Facebook's market power in the data market. A user who would not have freely given his/her personal data to Facebook is now doing so because this is a requirement for access to Facebook service. Thus, the requirement increases the market share of Facebook in the data market. Since the data is used to sell ads, Facebook's requirement directly increases its market power in the ads market, and stifles competition in this market. To the extent that a user is not compensated adequately for

[28] For an in depth analysis of this question, see ACCC, Digital Platforms Inquiry (June 2019), available at https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf , 8-10 & 89-99.

his personal data by the free provision of Facebook service, he is damaged by the requirement practice. Additionally, there are users who are willing to compensate Facebook for its service but would prefer not to provide their personal data to Facebook, who are damaged under Facebook's requirement.

How would the world be without this requirement? First, the default regime would be "opt-out," likely imposed by regulation since Google and Facebook do not have incentives to change the present opt-in default regime. In the opt-out regime, the company (Google or Facebook) is unable to legally use or sell the information it collects from a user who has not opted-in. To be able to use or sell information the company collects from a user, the user would need to affirmatively give his/her consent by opting-in. The user may demand compensation or be offered compensation for selling his/her data to the company, and opt-in occurs when a price has been determined and money changes hands.

So, a potentially vibrant market for personal information sold to Facebook or Google has been killed through the requirement practices of Facebook and Google that impose provision of personal data as a requirement for access to Facebook service or Google Internet search service. This is a "market failure" and can be fixed by antitrust and competition authorities in the US, EU and around the world. This goes beyond privacy concerns on the acquisition of personal information that are typically based on "rights" of individuals (for example, see *General Data Protection Regulation*, GDPR of the EU) rather than failure of markets and antitrust violations.

We now briefly describe how the market for sale of personal user data may function once we depart from the arbitrarily-imposed zero price and the present market failure.

We expect that there is plenty of variation both in the company's willingness to pay for users' personal information and in the users' reservation price for the sale of their personal information; of course there is also variation in the willingness to pay for Google (or Facebook) service. In a competitive world, we would expect two different markets. In the case of Google the two markets would be, market one for Internet search, and market two for acquisition of personal information by Google. Similarly, for Facebook, the two separate markets would be, market one for Facebook social network service, and market two for acquisition of personal information by Facebook. When combining the total charges in the two markets, that is, price collected by Google or Facebook) in market one minus price paid by Google (or Facebook) in market two, we expect that some users would end up paying a positive price for Google (or Facebook) in total, some would be paid by Google (or Facebook) in total, and some would receive break even in total.

Additionally, issues of market operation and allocative efficiency arise because of Google's and Facebook's dominance in their respective markets. Even in a "default opt-out" regime, because of its market dominance, Google (or Facebook) can overcharge users or not pay them the competitive price to provide 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 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*, where Google has the possibility to perfectly price discriminate to induce the user to sell his/her personal information. 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 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 monpsonist in the acquisition of personal user information. This is a *no requirement regime with a perfectly price discriminating monopsonist*.

We assume that, when a user does not use search and does not provide data, he/she receives a benchmark utility normalized at zero, $U = CS = 0$. 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 utility and consumer surplus in the various actions and regime changes from these benchmarks. We assume that Google has zero marginal cost in search.[29]

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 utility and consumer surplus

$$U = CS = x - z,$$

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

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

[29] The marginal cost of an additional user for Google and Facebook is is very low (almost zero), especially when compared to their fixed costs.

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 utility. Google receives zero benefit as well.

If x < z: U = CS = 0, G = 0.

The current requirement regime results are summarized in Table 1.

Table 1: Present Regime: Default opt-in, Google provides search only if it collects personal data

		Benefit to user	**Benefit to Google**
x > z	User accepts the requirement, uses search and provides personal information	U = CS = x – z > 0	G = y > 0
x < z	User rejects the requirement, does not use search and does not provide personal information	U = CS = 0	G = 0

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. 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 the search, and can pay price p2 o the user for personal data provision.

Rivalry among Internet search companies drives the price in the Internet search market to zero p1 = 0,[30] resulting in

U = x, G = 0

from the participation in the Internet search market. Since the maximum benefit from personal data to Google is y, Google would be willing to pay up to p2 = y for personal data acquisition, resulting in benefit

G = y – p2.

Once the market for personal information is open from the requirement, other firms will bid up to $y to acquire the personal information of a user. Competition among them will result

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

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

$$U = x – z + p2 = x – z + y, G = 0.$$

This strategy works as long as $y > z$.

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 utility than when the user did not provide data, $U = x + y – z < x$ since the user had utility $U = x$ when not providing data. Therefore, if $y < z$, the user accepts no offer, resulting in

$$U = x, G = 0.$$

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

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

		Benefit to user	**Benefit to Google**
$y > z$	User provides data at price $p2 = y$	$U = CS = x + y - z > 0$	$G = 0$
$y < z$	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	$U = CS = x > 0$	$G = 0$

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 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**	$U = CS = x - z > 0$	$G = y > 0$	Yes, N/A
$z > x$	**Default opt-in, requirement, and user rejects**	$U = CS = 0$	$G = 0$	No, N/A
$y > z$	**Default opt-out, no requirement, user sells info**	$U = CS = x + y - z > x > 0$	$G = 0$	N/A, Yes
$y < z$	**Default opt-out, no requirement, user does not sell info**	$U = CS = x$	$G = 0$	N/A, No
$x > z$, $y > z$	**Change of benefit by the removal of the requirement**	$\Delta U = y > 0$	$\Delta G = - y < 0$	Yes, Yes
$x > z > y$	**Change of benefit by the removal of the requirement**	$\Delta U = z > 0$	$\Delta G = - y < 0$	Yes, No
$y > z > x$	**Change of benefit by the removal of the requirement**	$\Delta U = x + y – z > x > 0$	$\Delta G = 0$	No, Yes
$z > x$, $z > y$	**Change of benefit by the removal of the requirement**	$\Delta U = x > 0$	$\Delta G = 0$	No, No

In terms of participation in the provision of data to Google, all four possibilities arise: users who accepted the requirement and sell personal 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. [31]

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, $\Delta U > 0$, ΔG

[31] 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 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).

≤ 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.

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 ($z > x$, $z > y$). And among those 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 has the various features of a functioning economic market. For example, there is variation in the willingness to pay defining a demand curve, and, given an offer price by Google, some users participate in the market at the price offered by the buyer while others do not.

We have shown that a vibrant market for personal information sold to Google has been killed through Google's practice to imposes provision of personal data as a requirement for access to Google's Internet search service. This is a "market failure" and can be fixed by antitrust authorities in the US, the EU, and other jurisdictions.[32]

We have shown that users are worse off, and Google is better off under the requirement. Assuming that people can determine rationally if it makes sense to provide their data, absence of the requirement will lead to the users being paid by the digital platforms for harvesting of their data. Removing the requirement improves consumer surplus as the price of data is positive in its absence since users get paid for selling their data to the platform. Typically, this will also lead to more data being collected.

We now discuss 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 is able to charge a price for search and a second price for the provision of personal data. We assume that the price for search may not fully extract the benefit of search for the user, possibly because of competition with rival browsers. So, when the user uses Google Internet search but does not allow Google to use his/her 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

$U = CS = (1 - k)x > 0$ if $k < 1$, $G = kx$.

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

[32] The analysis for Facebook is very similar.

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

$$U = CS = x - z - p1 + p2 = x(1 - k) - z + p2,\ G = y + kx - p2$$

since 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 for search and pays p2 to the user for providing that data. Therefore, the benefit to Google is G = y + kx – p2.

If y > z, that is, if the value of the personal data of the user to Google is higher than the value of loss of privacy to the user, Google can offer up to $y and be better off than when no data is provided. Since Google is dominant and knows 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 make the user provide data, by making his/her utility slightly higher that U = x(1 – k), which is the utility of no data provision. Therefore, Google will offer to the user p2 = z to buy his/her data, resulting in:

$$U = x(1 - k) - z + z = x(1 - k) > 0,\ G = y + kx - z > 0.$$

Notice that Google's payment for personal data as a monopsonist 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 utility than when the user does not provide data:

$$U = x(1 - k) - z + y < (1 - k)x.$$

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

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

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

<u>Table 4a:</u> 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

		Benefit to user	**Benefit to Google**
y > z	User provides data at price p = z	U = CS = x(1 – k) > 0	G = y - z + 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	U = CS = x(1 - k) > 0	G = xk

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

<u>Table 4b</u>: Comparison of the status quo to opt-out default 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**	U = CS = x - z > 0	G = y > 0	Yes, N/A
z > x	**Default opt-in, requirement, and user rejects**	U = CS = 0	G = 0	No, N/A
y > z	**Default opt-out, no requirement, user sells info**	U = CS = x(1 -k) > 0. When k = 1, U = 0	G = y – z + xk > kx. When k = 1, G = y – z + x > x	N/A, Yes
y < z	**Default opt-out, no requirement, user does not sell info**	U = CS = x(1 -k) > 0. When k = 1, U = 0	G = xk. When k = 1, G = x	N/A, No
x > z, y > z	**Change of benefit by the removal of the requirement**	ΔU = z – kx . When k =1, ΔU = z – x < 0	ΔG = - z + xk < 0. When k = 1, ΔG = – z + x > 0	Yes, Yes
x > z > y	**Change of benefit by the removal of the requirement**	ΔU = z – kx < 0. When k =1, ΔU = z – x < 0	ΔG = - y + xk. When k = 1, ΔG = x – y > 0.	Yes, No
y > z > x	**Change of benefit by the removal of the requirement**	ΔU = x(1-k). When k =1 ΔU = 0.	ΔG = y- z + kx. When k = 1, ΔG = x – z < 0.	No, Yes

z > x, z > y	**Change of benefit by the removal of the requirement**	ΔU = x(1-k). When k =1 ΔU = 0.	ΔG = xk. When k = 1, ΔG = 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)**	U = CS = x(1 - k) > 0. When k = 1, U = 0	G = y – z + xk > 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)**	U = CS = x + y - z > x > 0	G = 0
y < z	**Default opt-out, no requirement, user does not sell info, G monopsonist (regime 3)**	U = CS = x(1 - k) > 0. When k = 1, U = 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)**	U = CS = x	G = 0
y > z	**Change of benefit from 3 to 2 (2 minus 3)**	ΔU = x + y – z - x(1 -k) = y – z + xk > kx > 0	ΔG = -(y – z + xk) < -xk < 0
y < z	**Change of benefit from 3 to 2 (2 minus 3)**	ΔU = x - x(1- k) = kx > 0	ΔG = - kx < 0.

Table 5 shows clearly that competition in the personal data market makes users better off and Google worse off in comparison to Google being a monopsonist in the personal data market. This is as expected. It underlines the fact that removing the requirement is not sufficient.

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

2.2. Natural monopoly or natural oligopoly and market failure in privacy

Contrary to the repeated statements by some,[33] Internet search exhibits network effects because a higher number of search queries improve the quality of search of the particular search engine.[34] Thus, the higher market share of Google in search increases the quality and value to a user of Google's search. This is direct evidence of network effects: higher market share of the service increases the value of the service to the user. Also, when data provision is required for search, the more users you have, the more data you collect, and therefore the company can sell more valuable ads.

Google's requirement of personal data provision to receive Internet search implies that as more people use Google search, Google receives more personal data. So, Google uses its large market share in search in combination with the requirement to increase its market share in data (and enhance its dominant position). As we explained in the previous Section, the requirement increases the ability of Google to refine its categorization of a person, thereby increasing the amount that advertisers are willing to pay. This increases its profitability.

Data collected directly from the individual user, data from the location of the individual, data from Google's virtual assistant Alexa, publicly available data (for example Census data), and data bought from data brokers are combined by Google to refine data sold directly to advertisers and other intermediaries. Google would not have paid for such data had these been not useful and their usefulness is the complementarity they offer in order to make better predictions.

Size and high market share matters for both advertised-based platforms, Google and Facebook. First, we have the direct network effect of adding a user to Google because the addition improves search results for every Google user (and the addition of a Facebook user improves the Facebook experience for all users). Additionally, the requirement of personal data provision to receive Internet service improve the accuracy of data that Google and Facebook sell to advertisers and help increase the market share of each of these companies in the advertising market. So,, the more users you have, the more the users you have in search, the more the advertisers you attract on the other side, and the more valuable it is for the advertisers to use Google on the other side.

Traditionally network effects are defined as pertaining to the demand side of the market, while increasing returns to scale is a term reserved for decreasing unit cost at constant quality in production. Here, the scale of operation and the quality level of the company in the advertising market both increase with the provision of personal data by more users. More users are providing personal data under the requirement aiming to reap the direct network effects in search. The requirement implies that higher scale in consumption of Google's Internet search

[33] See, H.R. Varian, Use and Abuse of Network Effects (September 17, 2017), available at SSRN: https://ssrn.com/abstract=3215488 ; C. Tucker, Why Network Effects Matter Less Than They Used To, Harvard Business Review (June 22, 2018), available at https://hbr.org/2018/06/why-network-effects-matter-less-than-they-used-to .

[34] This is particularly true for idiosyncratic queries (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.

results in higher quality in the advertising market. The requirement transforms a purely demand-side network effect to a supply-side effect.

With regard to advertisers/data brokers, Google may have monopsony power at the brokers side, in comparison to Microsoft, therefore they can buy the data more cheaply, thus reinforcing their monopsony and monopoly with regard to advertisers

With regard to users, Google is also monopsony for the users even if it does not charge them. As shown earlier, we expect to have higher participation of users selling their data to Google under untying. That could have been positive if that was a traditional monopsony, but this market is not a traditional monopsony because, under tying, Google fixed the market price to zero rather than it being determined as in the traditional monopsony model (endogenous determination). Additionally, under untying, Google offers personalized pricing, again deviating from the traditional monopsony model.

We showed at the previous Section that users are worse off and Google is better off under bundling. Assuming that people can determine rationally if it makes sense to provide their data, a competitive market in the data collection from users, will lead to the users being paid by the digital platforms for the harvesting of their data. Unbundling improves consumer surplus over bundling as the price of data is positive under unbundling since the users get paid for selling their data to the platform and this will also lead to more data being available and collected.

Note that someone that values privacy as a deontological principle (values the idea of privacy) would find problematic that users have the possibility to share their own data, and would be in favour of suppressing data output. In this case a monopsony may not be welfare reducing. 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 may not be easily assessed. They may be inclined to share data, in particular if they receive payment for this, which they may likely regret, had they considered their long term interests. The above could build a behavioural economics critique to the idea that consumers should be paid for their data, and build an argument that monopsony might be efficient, from a social welfare perspective.

An argument could thus be made for nudging users to opt out, rather than to select to receive rewards/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 (private monopoly) so as to replace it with a ‘public interest’ motivated monopsonist, which would limit the harvesting of data to what is absolutely necessary for the improvement of the service to the user (hence, the full consumer surplus would go to the user). However in this case, there may be some costs to innovation. This may be avoided if this state-owned monopolist has the obligation to share data in situations in which this will lead to socially useful innovations by complementary firms, and therefore the social value of information outweighs the social cost of the loss of privacy for the individual user. There is always a risk that determining what is ‘socially useful’ would be sub-optimal if this is done by a regulator or a state monopolist in view of the discretion offered to the regulator/state-owned monopolist and consequently the risk of capture and inefficiency (this is a classic criticism to the administered economy). Hence, some other system of determining what is socially useful may be more preferable. Some authors have put forward quadratic voting as a procedure to overcome the tyranny of the

majority (here citizens that are indifferent to the protection of their privacy) and provide proportional weight to people whose interests in a social outcome are stronger (people that greatly value privacy).[35] Quadratic voting is not subject to the criticisms by Arrow to the voting theory of welfare for collective decision-making in order to determine the 'will of the people,' as it does not assume ordinal preferences as Arrow in his impossibility theorem.

One may also refer to historical patterns in the industry in order to assess how rising concentration and dominance may have found their source in conduct and business strategies harming privacy, rather than competition on the merits, or may have reinforced the dominant position of the firm by erecting important barriers to entry through the control of important amounts of data. With regard to the social media industry, Srinivasan argues 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. However, the landscape changed sharply in recent years, predominately because of the business strategy of Facebook.[36] Srinivasan narrates how Facebook initially entered the social media market in 2007 putting forward its 'superior' privacy-centered offer, linked to the fact that it was a 'closed communication network' requiring 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 the ability to opt-out of having their information shared with third-parties, including advertisers or marketers and promised them it would remove their information on demand.[37] Any effort by Facebook to track users' behaviour, through its advertising product Beacon, or subsequently social plugin products, was unsuccessful, as it led to users' backlash and Facebook had to withdraw the product and change its privacy policies, by including a commitment to allow users to vote on future changes that contractually change user privacy.[38] However, after a decade of 'false statements' and 'misleading conduct', reneging on previous promises not to track users, Facebook was able to leverage the superior information it has over its users in order to sell more advertising, with the result that the market for digital advertising has been transformed to a duopoly, dominated by Facebook and Google, the two companies accounting for 90-99% of year-over-year growth in the US digital advertising industry.[39]

Facebook also secured the cooperation of independent publishers and other businesses participating to its ecosystem, requiring all businesses to 'change their own privacy policies to extract from their own users the consent to have Facebook track them for commercial purposes.'[40] More importantly, the author claims that Facebook was able to change its privacy policy towards a more active use tracking, after it won against competing social networks, with rivals such as Snapchat and Orkut marginalized or excluded from the market, and consolidated its dominant position on the social media market, in particular during the period after 2014.

[35] E.A. Posner & E.G. Weyl, Voting Squared: Quadratic Voting in Democratic Politics, (Coase-Sandor Institute for Law & Economics Working Paper No. 657, 2014).
[36] D. Srinivasan, The Antitrust Case Against Facebook (September 10, 2018). Berkeley Business Law Journal Vol. 16, Issue 1, Forthcoming, available at SSRN: https://ssrn.com/abstract=3247362 .
[37] Ibid.
[38] Ibid.
[39] Ibid.,
[40] Ibid.

Hence, privacy-reducing policies were possible only because the users had no other choice of social network to switch to and were thus the direct result of Facebook's dominance on the social media market.

2.3. Lock in and Hold up

Research focusing on explaining the reasons that users would switch to a different social network from the one they currently used shows that users do not switch among social media providers for privacy reasons, but that such decisions are motivated by a number of different factors.[41] This research however dates from the period before the change of the dominant business model in social media in 2014, with Facebook moving to systematically monitoring and recording users' activity, as well as the backlash and the increasing awareness of users about issues of privacy and personal data protection, in particular following the Cambridge Analytica scandal[42]. Users may be less open to share information on social media and take increasingly action to monitor their browser data and the information they share.[43] Ad blockers have also gained in popularity. However, this has not greatly affected users' switching to more privacy-centred social media, nor has it led to the development of 'pay for privacy' business models, where users will pay for service with money rather than with their data.[44] Although not related as such to social media, research also shows that user inertia determined by 'cognitive, affective, and subconscious antecedents' may also play as a mooring factor and affect consumers' switching behaviour.[45] Identity network effects may also impact on the decision of users to switch, in particular if most of their friends are participating to the platform they want to switch from, hence creating sunk costs for the user if he decides to switch to a rival social media platform.[46] Such path dependency and the switching costs arising out from the buyer side contribute to the development of highly concentrated market structures. Single homing is also quite prevalent, in particular in view of the development of 'path dependent consumption,' with users developing consumption patterns which they are reticent to change, each additional consumption of the same product reinforcing the effect and leading to a quite strong loyalty effect, the user being emotionally or subconsciously locked in a specific product

[41] C. Zengyan , Y. Yinping & J. Lim, 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 (2009), available at http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.402.4797&rep=rep1&type=pdf ;

[42] See, https://www.wired.com/story/cambridge-analytica-whistle-blowers-and-techs-dark-appeal/ .

[43] See, https://www.emarketer.com/content/how-social-media-users-have-and-have-not-responded-to-privacy-concerns .

[44] See, https://www.emarketer.com/content/how-social-media-users-have-and-have-not-responded-to-privacy-concerns .

[45] Y. Sun, D. Liu, S. Chen, X. Wu, X-L. Shen, X. Zhang, Understanding users' switching behavior of mobile instant messaging applications: An empirical study from the perspective of push-pull-mooring framework, (2017) 75 Computers in Human Behavior 727.

[46] J. Mahmoodi, J. Čurdová, C. Henking, M. Kunz, K. Matić, P. Mohr & M. Vovko, Internet Users' Valuation of Enhanced Data Protection on Social Media: Which Aspects of Privacy Are Worth the Most?, (2018) 9 Front Psychol. 1516.

or digital platform, even if the choice is not optimal, in terms of quality or the amount of personal data harvested[47].

2.4. Information asymmetries and information related failures

Under complete information, the user knows (x) his/her valuation of Facebook's services. But is this really the case? At present, the user does not pay for the access to Facebook. Facebook is a 'free' product in terms of monetary payment. However, the user pays (has a cost) by providing personal data to Facebook for free. This may reduce the user's privacy or may enable the digital platform or whoever else is controlling this data to exploit the user in the future by personalised pricing etc. Hence, there is an issue of transparency of the full costs for the user of the engagement with Facebook. The user just sees the current monetary costs (zero) and does not take into account future costs. Behavioural economic literature on discounting, silver lining effect (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) may explain why we need to take seriously into account behavioural biases.

Our model also takes into consideration the cost of losing privacy. So, the user is willing to pay $x for using Facebook, but the take-it-or leave-it contract of Facebook implies that he will lose privacy that he values at $z. So, the net willingness to pay of a user under the present default opt-in conditions is $x-z. If the default was opt-out, the user would be willing to pay $x. In a behavioural setup, the user may underestimate the value of the loss of privacy.

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

Digital platforms argue that data harvesting and network effects also provide value to the users. However, it is not clear what is the exact value of the network effects from which benefit the users. But even assuming that the data is valuable because of network effects, it is difficult to determine the part of the value that represents the individual contribution brought by the data of the specific user. The user anyway gets better service as his data may enable the platform to provide more relevant queries in some cases and to improve the quality of search for tail queries. The issue is however if the platform collects more data than is needed for improving the service or the quality of the platform: the extra harvesting of data creates 'behavioural surplus' that will itself be highly valued in behavioural futures markets[48].

The lack of competition between networks does not provide information (transparency) about how much the user is valued by digital platforms, such as Facebook, so that the users could have information enabling them to bargain a 'better' deal. This leads to no surplus left for users as it affects the ability of users for collective action against the monopolist, for

[47] See, S. Lee, Economic Dependence on Online Intermediary Platforms and Its Exploitative Abuse (January 1, 2019). LL.M. Dissertation, Faculty of Law, University of Amsterdam, available at SSRN: https://ssrn.com/abstract=3343370 citing, *inter alia*, work by S. Siray, 'Combining marketing theory and path dependence' (Freie Universität Berlin 2016) and B.K. Schulte, *Staying the Consumption Course - Exploring the Individual Lock-in Process in Service Relationships* (Springer, 2015).

[48] See S. Zuboff, *The Age of Surveillance Capitalism* (Public Affairs, 2019).

.

instance by switching to a rival network. In any case, the choice may be quite limited, in view of the consolidation of the sector, and in particular the dominance of the advertised-based model.

To this, one may add the social costs of the lack of knowledge by the user of the broader social costs of letting their data being harvested by Facebook or Google: costs to democracy and pluralism, which may be an important concern, also for competition law, in some jurisdictions

2.5. Missing markets

The previous examples of market failure assume that there are privacy markets, but these operate inefficiently. One may however argue that the problem is more fundamental to the extent that there are no markets whatsoever. Contrary to the assumptions of the first fundamental theorem of welfare economics, there does not exist a complete set of markets for privacy, data or attention, which are demanded and supplied to be traded at publicly known prices. Actually, data is harvested by search engines for free, as users are not paid any compensation for the data they contribute, with the exception of the free use of the search engine, for which in any case the marginal costs are close to zero. The users cannot also determine what is the value of their data to the digital platform (e.g. Facebook), as they do not have access to the information on transactions between Facebook and advertisers at the other side of the platform. At the same time, the harvesting and use of their personal data may provide to users some benefits if they are offered targeted advertising (which may be positive in case one adheres to the information view of advertising) and a more personalised service. The price that advertisers pay Google or Facebook do not provide any further information as these transactions are not about the users' personal raw data but about inferences made on the basis of their data.

Hence, it appears that the digital economy is characterized by missing markets[49], because of the lack of property rights on personal data. Legal regimes may choose to protect entitlements by granting property rights, through a liability rule and regulation, or a combination of the two. If the situation is subject to liability rules, the violation of the specific entitlement to privacy without agreement, should lead to the compensation of the victim for the damages incurred. Property rights provide to their holder the right to legally bar, by injunctive relief, anyone violating his entitlement without his consent. The idea is that the violation of property rule is severely punished with injunctive relief (which is costly), thus deterring the violation of the entitlement at the first place and therefore avoiding future harms. A liability rule is more backwards looking as the aim is to compensate through damages for harm already done. A property rule will always be more favorable toward the injuree (the person whose entitlement is to be violated), and a liability rule will always be more favorable toward the injurer. Property rights also facilitate bargaining.

The allocation of property rights should nevertheless not impose an externality. This may be the case if providing property rights could, for instance, lead some to forego privacy for

[49] See, on the problem in general, G.M. Hodgson, How mythical markets mislead analysis: an institutionalist critique of market universalism, (2019) Socio-Economic Review**,** mwy049, https://doi.org/10.1093/ser/mwy049 .

instant gratification, with devastating long-term consequences, not only for them personally, but also for society overall. One may for instance envisage the social costs engendered by an entity that has induced users to provide freely, or sell their personal data, in order to manipulate them more easily, because of the reduction of the levels of privacy protection, and thus extract more surplus from users. As mentioned above the lack of property rights and therefore the missing markets issue may not allow parties to negotiate a Pareto efficient transaction. If such social costs are important, there is also an argument for banning such transactions, thus making personal data inalienable. In our view, the level of development of the digital economy does not render this a pragmatic option to follow at this stage.

The lack of a proper regime of property rights on personal data has important implications on the ability of users to protect their interests and capture a part of the surplus value they contribute to. At the same time, digital platforms are able to rely on a quite expansive definition of the domain of intellectual property law and contract law in order to impose almost unilaterally conditions to the users of their products, in practice challenging their autonomy and their freedom to use as they wish their tangible property. The lack of a proper property regime for personal data has enabled digital platforms to harvest this valuable raw material, without any corresponding protection of the interests of the users, by just relying on their consent to their terms and conditions. The possession of this data does not rely on a properly defined property regime (hence the distinction between possession and property rights) but on the control by these digital platforms of important bottlenecks in the way users access the Internet and the various services this may give them access to. The GDPR does not put in place a proper property rights regime for personal data, which would have granted formal rights sanctioned by a public authority, delimited the boundaries of these rights, or establish a system to adjudicate disputes as to the ownership of these rights. Having possession of the item, in the sense of physically controlling it, constitutes just one of the bundle of rights provided by property and ownership, 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, the possibility to use it as security in order to borrow against it. This is still not possible for personal data.

3. Exploitative and exclusionary conduct involving privacy-related theories of harm: ex ante and ex post enforcement

The development of the digital economy leads to an increasing interest of competition authorities for privacy-related theories of harm, both in *ex ante* and *ex post* enforcement. We will explore the various theories put forward and the limits of the existing legal tools to address these new theories of harm.

3.1. 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 is nonetheless a more complex issue, in particular in view of the *ex ante* nature of merger control and the possibility to address privacy restrictions of competition ex post through the enforcement of data protection laws. The possibility that a merger may be considered anticompetitive because it may lead to a substantial lessening of competition on privacy, or more broadly may have negative consumer welfare effects because of a restriction of the level of privacy in the market, was explored in some recent merger decisions in the EU and the US. As a starting point, we note that both US and EU merger guidelines explicitly recognize non-price factors of competition[51]. In both jurisdictions such factors may often be considered at the level of market definition, rather than at the later stage of determining theories of harm. However, as a recent OECD report notes, '(t)hese market definition approaches have not been explicitly applied in any merger case to date'[52].

We will focus here on the second issue, the first being relatively uncontroversial and not presenting anything specifically different than the traditional approach to mergers[53]. With regard to privacy concerns, the dominant view is to consider this as a parameter of competition in quality. In this context it can be integrated in the competition assessment under a 'consumer welfare' standard, broadly defined[54]. However, this approach may be subject to criticism[55], and is not the only available option, as we will examine in X.

Starting with the EU, in the *Facebook/WhatsApp* merger, a possible theory of harm explored by the 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'[56], thus strengthening Facebook's position in the provision of online advertising services as a result of

[50] See, for instance, M Stucke & A Grunes, *Big Data and Competition Policy* (OUP, 2016), chapters 6–8.

[51] See, for US Guidelines, U.S. Dep't of Justice and the Fed. Tr. Comm'n, Horizontal Merger Guidelines §4.0 (2010), available at https://www.ftc.gov/sites/default/files/attachments/merger-review/100819hmg.pdf (noting 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' and that '(w)hen the 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 .

[52] OECD, Considering non-price effects in merger control – Background note by the Secretariat, DAF/COMP(2018)2 ¶112.

[53] See, for instance, the US submission to the OECD's workshop on Non-price effects of mergers, ¶9 (noting that '(e)vidence 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').

[54] For a discussion, see OECD, 'The Role and Measurement of Quality in Competition Analysis' DAF/COMP(2013)17 <http://www.oecd.org/competition/Quality-in-competition-analysis-2013.pdf> accessed 21 October 2018. The existence of a trade-off between these various parameters of competition protected by the 'consumer welfare standard' is an open question, in particular as 'the superficial consensus' on consumer welfare 'masks a deep disagreement about what 'consumer welfare' means and especially about what policies best to promote it': G Werden, 'Consumer welfare and competition policy' in J Drexl, W Kerber and R Podszun (eds), *Competition Policy and the Economic Approach: Foundations and Limitations* (Edward Elgar 2011) 15

[55] See, the discussion in OECD, Considering non-price effects in merger control – Background note by the Secretariat, DAF/COMP(2018)2 ¶¶ 113-119.

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

the increased amount of data which will come under Facebook's control.[57] However, the Commission found no concern with regard to the strengthening of Google'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 collected user data alongside Facebook, not least Google. This left, according to the Commission, a large amount of Internet user data that are valuable for advertising purposes outside Facebook's exclusive control.[58] However, the Commission did not take sufficiently into account the possibility that the data collected by Double/Click, which contained information about a rich sub-set of the web-browsing behaviour of Double/Click users across all publishers' websites engaged in targeted advertising, could facilitate online price discrimination, enhancing the power of the entity to exploit consumers. The Commission accepted DoubleClick's justification that it collected behavioural data from its users for only legitimate purposes, such as improving the overall experience offered to advertisers, and the fact that these were aggregate data that could 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 to switch to alternative ad serving providers in case Doubleclick violated the confidentiality provisions[59]. The Commission unconditionally cleared Google's acquisition of DoubleClick finding 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 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'[60].

However, the Commission did not focus on the exploitation concerns, dismissing the possibility that the acquisition of WhatsApp by Facebook would enable Facebook to use WhatsApp user data to better target Facebook ads, the Commission doubting on whether Facebook would have the ability and the incentive to engage in such conduct post-transaction. The impact of the merger on privacy was also sidelined. According to the Commission, '(a)ny privacy-related concerns flowing from the increased concentration of data within the control of Facebook as a result of the Transaction do not fall within the scope of the EU competition law rules but within the scope of the EU data protection rule.'[61] The Commission focused on the exclusionary/anticompetitive foreclosure related concerns, leaving any possible exploitation concerns, in terms of impact on users' privacy to be dealt by data protection law.

In August 2016, WhatsApp updated its privacy policy to allow for linking WhatsApp users' phone numbers with Facebook users' identity. Hence, the previous statement at the time of the assessment of the merger was proven to have been misleading. Indeed, at the time the

[57] Ibid., para 184.
[58] Ibid., para 189.
[59] Ibid, para 277.
[60] Ibid, para 360.
[61] Ibid, para 164.

merger transaction was assessed, Facebook had offered assurances to the Commission, both in the notification form and in a reply to a request of information, that it would be unable to establish reliable automated matching between Facebook users' accounts and WhatsApp users' accounts. The Commission imposed a €110 million fine on Facebook for providing misleading information about the WhatsApp merger[62]. It also found that, contrary to Facebook's statements in the 2014 merger review process, the technical possibility of automatically matching Facebook and WhatsApp users' identities already existed in 2014, and that Facebook staff were or should have been aware of such a possibility[63]. However, this did not affect the Commission's authorisation of the merger as the clearance decision was based on a number of elements going beyond automated user matching.

In *Microsoft/Linkedin*, the Commission raised two types of concerns relating to data combination.[64] One of the theories of harm was that the merged entity could integrate LinkedIn into Microsoft Office and thus combine, to the extent allowed by contract and applicable privacy laws, LinkedIn's and Microsoft's user databases, giving Microsoft's the possibility to shut out its competitors in the customer relationship management market. In particular, Microsoft could deny its competitors access to the full LinkedIn database, and thus prevent them from developing advanced customer relationship management functionalities also through machine learning. The Commission was not however convinced that access to the full LinkedIn database was essential to compete on the market and held that LinkedIn's product was not a 'must have' solution.[65]

The second theory of harm was more directly concerned with data concentration and its effects on online advertising services. The Commission explored how the regulatory framework in the EU relating to data protection could mitigate some of the competition law concerns:

> '(177) As a preliminary remark, it should be noted that any such data combination could only be implemented by the merged entity to the extent it is allowed by applicable data protection rules. In this respect, the Commission notes that, today, Microsoft and LinkedIn are subject to relevant national 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. Currently, the data protection rules of the EU Member State(s) where Microsoft and LinkedIn have their registered seat and/or where they have subsidiaries processing data apply. […]
>
> (178) Moreover, the Commission notes that the newly adopted General Data Protection Regulation ('GDPR')[66] […] provides for a harmonised 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. This may further limit Microsoft's

[62] Facebook/WhatsApp, (Case COMP/M.8228), Commission Decision (May 17, 2017), available at http://ec.europa.eu/competition/mergers/cases/decisions/m8228_493_3.pdf .
[63] Ibid, para 86.
[64] Ibid., para 400.
[65] Ibid., para 277.
[66] General Data Protection Regulation (EU) 2016/679 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.

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 (i.e. easier access to personal data; right to data portability; etc.).'[67]

In view of the GDPR, the Commission found that it was not likely that Linkedin data could become in the next two to three years an important input in this market and that in any case, LinkedIn's privacy policy allowed it to share the personal data it collects, processes, stores and uses with third parties.[68] Again in this merger, the Commission refused to consider exploitation concerns arising out of the higher concentration of data and the combination of Linkedin and Microsoft's user databases, noting 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 her or his email or other contacts, search behaviour etc. about the users of their services) held by each of the (p)arties in relation to online advertising'[69]

Higher concentration of data could nevertheless have a potential impact to competition. The Commission found that the merger could lead to the marginalisation of XING, a competitor of Linkedin which offered a greater degree of privacy protection to users than LinkedIn (or making the entry of any such competitor more difficult), therefore restricting 'consumer choice in relation to this important parameter of competition.'[70] To address the competition concerns identified by the Commission in the professional social network services market, Microsoft offered a series of commitments, which the Commission found to address the competition concerns identified and therefore conditionally cleared the merger. This case offers the possibility to conceptualise privacy as a parameter of competition that may eventually be subject to measurement[71].

Privacy related theories of harm were also discussed in the recent merger between Apple and Shazam involved two companies providing complementary services (software solutions platforms and digital music streaming services for Apple and music recognition apps for Shazam)[72]. The Commission explored if the fact that Shazam currently collects certain data on users of third party's apps, and in particular digital music streaming apps, installed on the same smart mobile devices where the Shazam app is installed (for both Android and iOS devices) and allows those of its users who are also users of Spotify to connect their Shazam account (anonymous or registered) to their Spotify account (freemium or premium), therefore 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[73] could

[67] Ibid., paras 177–178.
[68] Ibid., para 255.
[69] Ibid, para 176.
[70] Ibid., para 350. Indeed, the Commission had found that privacy was an important parameter of competition and driver of customer choice in the market for professional social networking services.
[71] K Bania, 'The role of consumer data in the enforcement of EU competition law' 2018 (January) European Competition Journal; E Deutscher, How to Measure Privacy-Related Consumer Harm in Merger Analysis? A Critical Reassessment of the EU Commission's Merger Control in Data-Driven Markets (2017). Faculty of Law, Stockholm University Research Paper No. 40. Available at SSRN: https://ssrn.com/abstract=3075200 .
[72] Commission Decision, M.8788 - Apple / Shazam (November 11th, 2018), available at http://ec.europa.eu/competition/mergers/cases/decisions/m8788_1279_3.pdf .
[73] Ibid., para 199

have 'a negative impact on competition'[74]. 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[75]. Without entering into an in-depth assessment, from the perspective of data protection law (GDPR), the Commission proceeded to an abridged analysis of Shazam's terms of service and privacy Notice to conclude that the purpose of this harvesting of personal data has been specified and made manifest to Shazam's users. The Commission also referred to the EU rules dealing 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[76]. 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, thus enabling Apple to lawfully store or have access to this customer information. Possible contractual limitations to the use of this data could emanate from the Android Developer Guidelines, which so far had provided Shazam access to data about which apps are installed on a user's Android device, or by rivals to the new entity, such as Spotify, which, according to their developer terms and conditions of service, 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[77]. Notwithstanding these limitations, the Commission found that the new entity could collect this customer information lawfully and proceeded to the analysis of the incentive and ability of the new entity to use this customer information to put competitors at a competitive disadvantage[78].

In the US, harm to privacy did not come up in the context of assessing merger activity, any issues being dealt with through Section 5 of the FTC Act condemning unfair or deceptive acts or practices in or affecting commerce.

3.2. Ex post enforcement: abuse of a dominant position or economic dependence

Restrictions on privacy may also be subject to *ex post* enforcement, in particular, but not exclusively the prohibition of an abuse of a dominant position[79]. We explore different theories

[74] Ibid., para 219.

[75] Ibid., para 225. The Commission indeed 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 that '(d)ata 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., para 229.

[76] Ibid., paras 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 (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 his or her consent following clear and comprehensive information about the mature of data processing.

[77] Ibid., para 237.

[78] Ibid., para. 238.

[79] It is also possible for agreements that restrict competition on privacy to also fall under the prohibition of anticompetitive collusive practices, to the extent that such an agreement will reduce competition on a parameter of competition, quality, which in some markets may be a quite significant factor of the competitive game. This is well accepted now for agreements restricting innovation, and it should be the same for agreements restricting privacy. To the extent that an agreement to restrict competition on privacy may not have any redeeming virtue,

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

3.2.1. Excessive data extraction

'Excessive' data extra may constitute a competition law concern for some competition law regimes to the same extent that excessive prices have been targeted by some competition authorities.

It is worth noting that excessive pricing as a competition law issue has been a quite controversial topic, with certain jurisdictions, in particular the US rejecting the possibility to bring an excessive pricing case when this may only be motivated by concerns about exploitation, rather than by concerns about collusion. Despite the recent extension of the scope of Section 5 FTC Act to some forms of hybrid excessive/exploitative practices in the context of Standard Setting Organizations (SSOs) or related to SEP royalties, in the presence of a previous commitment of the dominant firm to license essential proprietary technology on RAND terms[80] or in breach of the duty of good faith of a member of an SSO with regard to the standardisation process[81], US antitrust law does not apply to purely exploitative practices. Although this had always been the case,[82] it has been made clearer in *Verizon v Trinko*, the Supreme Court noting that "(t)he mere possession of monopoly power, and the concomitant charging of monopoly prices, is not only not unlawful; it is an important element of the free-market system. The opportunity to charge monopoly prices – at least for a short period – is what attracts "business acumen" in the first place; it induces risk taking that produces innovation and economic growth."[83]

However, in the EU, and several other jurisdictions excessive pricing forms a well-accepted cause of action in competition law. In the EU, excessive prices may be found to infringe Article 102(a) TFEU which may apply to purely exploitative conduct (exploiting consumers directly without any requirement to prove any exclusionary conduct), in particular conduct that is 'directly or indirectly imposing unfair purchase or selling prices or other unfair trading conditions.'

---

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 qualifies it as a restriction of competition by its nature, without any need to assess its anticompetitive effects in great detail. It remains, however, an open question if agreements of this sort between undertakings with relatively low market shares, or in a non-concentrated market, may be a cause of concern justifying the (rebuttable) presumption of anticompetitive effect that would result a qualification of such agreements or concerted practices 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, most recently, Case C-179/16, F. Hoffmann-La Roche Ltd and Others v Autorità Garante della Concorrenza e del Mercato, ECLI:EU:C:2018:25, paras 79-80.

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

[81] See, *In the matter of Rambus, Inc.* (August 2, 2006), Docket No. 9302, pp. 34-35 available at http://www.ftc.gov/os/adjpro/d9302/060802commissionopinion.pdf ; *Rambus Inc. v. FTC*, 522 F3d 456 (DC Cir. 2008), *cert. denied*, 129 S. Ct. 1318 (2009).

[82] See, for instance, *Berkey Photo, Inc v. Eastman Kodak Co., 603 F2d 263, 294 (2nd Cir. 1979), cert. denied*, 444 US 1093 (1980).

[83] Trinko case.

One may argue that similar principles could apply to an 'excessive' extraction of data. However, as Haucap explains 'data is not like money', as it 'does not reduce the user's ability to provide the same data to another service of multiple other services'; this is 'a fundamental difference to excessive pricing cases where customers are left with less money/wealth once they have been exploited.'[84] As the German competition authority (Bundeskartellamt – BKA) has noted in its recent Facebook decision, '(p)ersonal data represent 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.'[85]

This analysis nevertheless ignores the impact data extraction may have on the reduction of privacy, not only because of the violation of the fundamental right of privacy but also from a purely user surplus perspective, to the extent that it enables the platform to predict the preference map and consequently the behaviour of the user. This provides the platform a structurally more powerful position in its future interactions with the users and the ability to reduce consumer surplus (not only in terms of not satisfying the privacy preferences of users, but also in reinforcing the platform's capacity to impose different price discrimination strategies against them)[86]. As the BKA also explains in its decision, 'the main problem' in the excessive extraction of data cases is that 'when consumers share their personal data, they are not really able to judge which and how many data are being collected by which company, to whom their data is being transmitted and what the implications of giving consent to data processing are.'[87] Users may be unaware that the extracted data is likely to facilitate their exploitation. The issue here will therefore be to decide if a prophylactic intervention focusing on excessive data extraction so as to avoid future instances of exploitation (eventually through different forms of personalised pricing and price discrimination) may be the preferable 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, note that this will require also some re-conceptualisation of price discrimination in competition law, which is not usually prohibited as such.[88]

Alternatively, privacy may be considered as a personal good valued by the consumer, and therefore any privacy reduction may be tantamount to a form of consumer harm (reduction of quality). One may argue 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 'excessive' enough by the user, or that he values the services provided by the platform more than the inconvenience of reduced privacy, to the extent that the exchange is voluntary and from this exchange and the 'price' in terms of privacy reduction the user is ready

[84] See, J. Haucap, Data Protection and Antitrust: New Types of Abuse Cases? An Economist's view in light of the German Facebook Decision, CPI Antitrust Chronicle (February 2019), 1.

[85] See, Bundeskartellamt, Facebook decision (2019), available at https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Entscheidungen/Missbrauchsaufsicht/2019/B6-22-16.pdf?__blob=publicationFile&v=5 , para. 571.

[86] J. Haucap, Data Protection and Antitrust: New Types of Abuse Cases? An Economist's view in light of the German Facebook Decision, CPI Antitrust Chronicle (February 2019),

[87] Ibid., para. 571.

[88] See, however, the Robinson Patman Act of 1936 in the US, which prohibits sellers from engaging in price discrimination. In the EU, price discrimination may violate the Treaty provisions, essentially for considerations relating to market integration purposes.

to pay reveal his real preferences about the trade of. This assumes that the user is fully informed about the reduction of his privacy and that he is rationally proceeding to a trade of between the costs and benefits of using the platform. However, although early studies found that individuals will perform a 'privacy calculus' before disclosing information necessary to complete an e-commerce transaction, more recent work has shown that there is some cognitive dissonance between consumers' online behaviour (their revealed preferences) and their stated preferences for privacy, leading to the so called 'privacy paradox.'[89] Users may value privacy, but do nothing to protect it.[90] Recent research also highlights the bounded rationality of consumers when performing this privacy calculus – in other words, consumers lack the bandwidth to compare the costs and benefits of sharing personal information.[91] The 'privacy paradox' is indeed a complex phenomenon the apparent discrepancy of people's concerns over their privacy and their online behaviours, such as bounded rationality, cognitive biases and heuristics, or social factors[92]. Further, 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' Terms and Conditions (T&Cs) of service due to length, legalistic language and a 'take it or leave' it approach.[93] For want of any better alternative, 'tick, click and hope for the best' sums up most consumers' attitude[94]. Through IoT users may in the future allow smart devices to engage in online transactions on their behalf based on learned preferences. A more systematic use of digital assistants might require default or adapted consent mechanisms.[95] Conversely, tech advances could lead to better results for consumers if, for

[89] A.C. Acquisti, R. Taylor & L. Wagman, The Economics of Privacy, (2016) 54 Journal of Economic Literature 442; V. Benndorf & H.-T. Normann, The Willingness to Sell Personal Data, (2018) 120 Scandinavian Journal of Economics 1260..

5 See Norberg P. A., D. R. Horne & D. A. Horne (2007), "The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors," Journal of Consumer Affairs 41, pp. 100-126.]

[90] S Barth, M DT de Jong, The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review, (2017) 34(7) Telematics and Informatics 1038.

[91] Acquisti et al (2013 and 2016) suggest that consumers often prefer short term discounts over long term risk of disclosing personal information. John, L. K., & Loewenstein, G. (2013). What is privacy worth?. The Journal of Legal Studies, 42(2), 249-274 and Acquisti, A., Taylor, C., & Wagman, L. (2016). The economics of privacy. Journal of Economic Literature, 54(2), 442-92.

[92] For a literature review, see S. Kokolakis, Privacy attitudes and privacy behaviour: a review of current research on the privacy paradox phenomenon, (2017) 64 Computers & Security 122.

[93] See, for instance, the meta-study by J. Mou, D.-H. Shin and J. Cohen, "Trust and Risk in Consumer Acceptance of E-Services", (2017) 17(2) *Electronic Commerce Research*, 255; A recent CUTS International survey on privacy and data protection in India covering 2,400 respondents revealed that around 80 percent users were not reading privacy policies. Key reasons for the same were such policies being lengthy, language barrier, and too much legalese. see http://www.cuts-ccier.org/pdf/Advocacy-CUTS_Comments_on_the_draft_Personal_Data_Protection_Bill2018.pdf .

[94] See also, J. Farrell, Can Privacy be Just Another Good?, (2012) 10 Journal on Telecommunications and High Technology Law 251, 257-259 (noting the existence of some form of confusopoly affecting the incentives of companies to improve privacy policies, as consumers are unable to observe better privacy policies, because of the complexity of terms and conditions, or have lost trust in the market to provide higher levels of privacy, with the result that the companies do not compete on better privacy terms, as consumers cannot reward their effort, preferring to obfuscate their privacy policies and thus confuse consumers).

[95] See, G Contissa et al, Towards Consumer-Empowering Artificial Intelligence, Proceedings of the Twenty-Seventh International Joint Conference on Artificial Intelligence Evolution of the contours of AI. Pages 5150-5157. https://doi.org/10.24963/ijcai.2018/714 .

example, artificial intelligence formed by learned consumer patterns was used to form buyer coalitions to seek better terms.[96]

The main difficulty with the excessive data extraction claim is to determine what constitutes '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, as this is determined either by using a cost+ approach, that is adding up the different costs of the product, or by comparing the price with a comparable competitive market, which should the preferred method in the context of an intangible economy. In the case of excessive data extraction, the counterfactual may more easily be established as the level of privacy enjoyed by the user in the absence of the specific conduct that is assessed as excessive. But one can also imagine a more abstract counterfactual which may broadly serve as the standard to determine the 'excessive' nature of the data extraction. This will relate to the purpose of the data extraction and how this affects the user's experience and therefore the 'quality' of the service provided. One may argue that the data extraction by the platform should not be considered 'excessive' if the data is used, either to improve the product in order to respond to the needs of the specific user, if personalisation is welfare-enhancing, or in case the platform is employing an advertised-based model to better match advertisers and consumers, which improves the situation of the user in comparison to what would have been the case had the user receive advertising of little interest to him. Consumers may indeed prefer to receive advertising that matches their preferences and could inform them about the products they are interested in, rather than 'junk' advertising.

Haucap observes that the 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'[97]. Certainly, this is behaviour that may fall under data protection or consumer protection rules, but as previously discussed the problem is exacerbated in case the platform has market or bargaining power and thus the consumer may not easily switch to an option that is more respective of his 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'[98]. Indeed, excessive data extraction will be an issue for competition law only in situations in which the platform disposes 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 could be considered as excessive. Some authors raise questions as to the legitimacy of such 'differential treatment' and the higher duties imposed on dominant undertakings.

[96] Some have coined the term 'algorithmic consumer' to convey the complexity of the decision process in the digital era of the Internet of Things ('IoT'): M. Gal and N. Elkin-Koren, , "Algorithmic Consumers" (August 8, 2016). Harvard Journal of Law and Technology, Vol. 30, 2017. Available at SSRN: https://ssrn.com/abstract=2876201.

[97] J. Haucap, Data Protection and Antitrust: New Types of Abuse Cases? An Economist's view in light of the German Facebook Decision, CPI Antitrust Chronicle (February 2019), 3.

[98] Ibid., 4.

We consider that these arguments do not stand serious scrutiny. First, only dominant undertakings are also targeted by provisions against excessive pricing, other undertakings being free to decide their pricing strategies. If this is not considered a problem for excessive pricing claims, it should not also be an issue for excessive data extraction claims. Second, as previously discussed a concentrated market constitutes a less optimal, from a privacy perspective, market structure than a less concentrated market, as there is a higher likelihood that the market tips to less-privacy centred business models, in particular in view of the higher valuation of advertised-based platforms by financial markets. Thirdly, it is in fact the preeminent position of the platform in its core activity and in adjacent markets that enables it to impose to its users a business model reducing their privacy, as the users cannot easily switch 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, which impose specific duties to all undertakings (and data comptrollers) irrespective of market size to protect the privacy of their users. However, there is also added value in competition law intervention.

It is likely that excessive data extraction may constitute a form of exploitative behaviour. There has been some discussion over targeting purely exploitative behaviour through the abuse of dominant position provisions. Commentators have expressed a number of reservations on this issue with regard to claims of excessive pricing, and it is important to explore if the same objections may also apply in the event of a privacy related harm:

(i) It is often acknowledged that determining excessive pricing may be hard, in particular determining the right benchmark. Would the perfect competitive price constitute such a benchmark? But what would that mean in the context of a market characterized by network effects? Can one assume that the but-for scenario would have been the development of a duopoly, or should we use models of imperfect competition? How can it be calculated? If one allows some margin above competitive price, what is the magnitude of this margin? How to establish reasonable return on investment?

(ii) Setting clear rules for compliance in dynamic markets is even harder; How should these rules apply in dynamic markets, where there is upfront investment for the future? Should one require high *ex post* margins to incentivise *ex ante* risky investments (e.g. in R&D)? It is important to acknowledge that high margins on some activities may be required to cover fixed costs that are common across activities;

(iii) Remedies for excessive pricing can equate to price regulation (either implicitly or explicitly);

(iv) Price regulation can be distortive to competition, investment and R&D; Price regulation can inhibit entry/expansion by competitors, can distort investment incentives, can distort incentives for marketing and R&D – i.e. 'portfolio pricing' approach (in view of the fact that the majority of R&D projects fail), may distort pricing incentives; Proponents of this view suggest that there may need to be explicit regulation for certain areas of natural monopoly – such as utilities – but this should be done carefully by sector-specific regulators. The rest of the economy should be left alone – since the risks of careless and ill-informed intervention outweigh any potential benefits;

(v) The problem will typically solve itself, since high profits encourage entry.

(vi) Defining what constitutes an excessive price is too complicated for competition authorities or the courts, which are not the adequate institutions for this task.

In view of these difficulties, commentators have suggested a number of limiting principles to the application of abuse of dominance provisions to purely exploitative practices, that should apply only in narrow circumstances, such as that there are very high and long lasting barriers to entry (and expansion); and the firms (near) monopoly position has not been the result of past innovation or investment[99].

However, from the above considerations, very few apply in the situation of excessive data extraction.

First, 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 to the data protection regulation, should this exist, can be presumed to be of an excessive level. From then on it is a matter of a case-by-case analysis of the specific conditions of the market in order to determine if the dominant position and the data policies adopted by the dominant platform contributed to the lower level of data protection and privacy, in comparison to the situation in the market before such dominant position emerged and the data policies altered. This case-by-case analysis of the conditions of the market and the business strategies of the firms is commonplace in competition law analysis.

Second, the risk of data extraction strategies is that once tried they may generate superior 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 that may be highly valued by financial markets. There is therefore a risk that the mode of competition and innovation in the industry will get stuck to an equilibrium that would be suboptimal from a data protection perspective. The difficulties mentioned above regarding fixed costs are not also that relevant in this context, in view of the multi-sided markets context of the business strategies followed, the non-price harm to consumers in this case in terms of reduced privacy being on a different market than the price effect, which is in the advertising market(s).

Third, the remedies for excessive data extraction may be straightforward and a cease and desist order would be in most cases sufficient to deal with the harm. Hence, there is no need for price regulation. Of course, if the remedy involves the requirement to offer users to pay for a more compatible to privacy option, determining the 'price' of privacy might require some form of price regulation. We explore the way this can be done in the last Section.

Fourth, any remedies aiming to promote data protection and privacy for users will most likely not distort competition, innovation and R&D. On the contrary, that may enable a differentiation of the business models followed by the platforms and nudge the direction of innovation efforts to models promoting privacy.

Fifth, it is not clear if the problem may solve itself, as once a market has tipped to a sub-optimal equilibrium in terms of privacy, for instance if platforms based on the advertised-based model harvesting personal data dominate the market, we have seen that it is quite difficult

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

for any platform to challenge this position, even if it offers a more privacy-enhancing alternative, in view of the network effects. Hence, some form of state intervention is needed. Sixth, determining if a platform has proceeded to an excessive extraction of data, including committing a violation of data protection law is certainly a much easier task for the courts than determining if a price is 'excessive', the latter involving some sophisticated economic analysis.

One could also challenge the argument over the risks that such claims set for legal certainty, requiring the development of narrow limiting principles. Contrary to the situation of price related exploitation, courts and competition authorities can more easily set clear principles on the basis of existing rules of data protection law, or in case they do not exist on the basis of the hypothetical revealed preferences of consumers, either determined through 'willingness to pay' (WTP) surveys, or because consumers usually value less privacy if they are asked how much they are ready to pay for it, instead of how much they would like to be paid in order to lose it (Willingness to Accept, WTA), through other methods (e.g. hedonic pricing)[100].

We will briefly explore the constitutive elements of an excessive harvesting of data case as a competition law violation in order to see how the existing case law regarding excessive prices may apply in this context. The focus will be on the EU as it is the jurisdiction that serves as a reference for other jurisdictions, including some BRICS countries, which also sanction excessive pricing[101].

---

[100] A. Acquisti, J. K. Leslie & G. Loewenstein, What Is Privacy Worth?, (2013) 42(2) The Journal of Legal Studies 249, 268 (noting that 'individuals' preferences for privacy may not be as stable or as internally consistent as the standard economic perspective assumes' and finding that there is a 'gap between privacy WTP and WTA' and arguing 'against the uncritical use of privacy valuations that have used single methods—for example, only WTP or only WTA').

[101] In **Brazil**, despite the reference in Law 12.529/2011, art 36, III to conducts which arbitrarily increase profits, a pure case of excessive pricing will not succeed. A possible effect in welfare is generally part of the antitrust analysis. Therefore, a case based on exploitative abuse of prices is unlikely.

In **Russia**, to date, there are no relevant digital competition cases dealing with excessive pricing. The only applicable case is the case against the four main telecom operators (MTS, Vympelcom and Megafon) that were found to have breached Article 10 (1) (1) of the Federal Law on Protection of Competition (setting and maintenance of monopolistically high prices). FAS of Russia said that the revenues these companies received by increasing their roaming tariffs were higher "than the amount of costs and profit necessary for efficient execution of inter-operator roaming agreements". No other (digital) cases from Russia dealt with excessive pricing.

In **India**, if a dominant firm "directly or indirectly imposes unfair or discriminatory price in purchase or sale (including predatory price) of goods or services", it will amount to an abuse of dominance (section 4(2) (a) (ii)). Any possibility of excessive or unfairly low prices is covered under this provision.

Recognizing difficulties in determining whether a price is excessive, the Commission in HT Media case [*In re M/s HT Media Limited & M/s Super Cassettes Industries Limited*, Case No. 40/2011, available at https://www.cci.gov.in/sites/default/files/C-2011-40_0.pdf] observed that 'in the absence of the cost data it will be difficult, neigh impossible, to term the price charged by the opposite party at … as unfair being excessive solely on the basis that it is higher than the price charged by the competitors of the opposite party'.

As a recent note by the CCI to the OECD acknowledges, "(g)iven the challenges associated with assessment of benchmark 'fair price', followed by regulatory dilemma of associated trade-offs between static and dynamic efficiency, the Commission has rarely intervened in cases exclusively involving excessive pricing as the primary allegation. Even in cases where intervention has been made, the Commission has been averse to devising any pricing remedies": Excessive Pricing in Pharmaceutical Markets - Note by India, OECD, 2018; DAF/COMP/WD(2018)113.

In **China**, excessive pricing is prohibited under Article 17(1) of the Anti-Monopoly Law. The legal test is similar to that put forward in *United Brands*. The conduct is assessed according the following test: (i) whether the dominant business operator sells products at high prices or buys products at low prices; (ii) whether the price is unfair. In assessing the unfairness, the following factors shall be taken into consideration: (i) comparison with

The legal test for excessive pricing in the EU results from the seminal *United Brands* case, where the Court of Justice (CJEU) held that a price may be found excessive if it has no reasonable relation to the economic value of the product supplied.[102] According to the Court, this excess could, *inter alia*, be determined objectively if it were possible for it to be calculated by making a comparison between the selling price of the product in question and its cost of production, which would disclose the amount of the profit margin[103]. A two- step analysis is carried out: it has to be determined '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, whether a price has been imposed which is either unfair in itself or when compared to competing products.'[104] These two conditions (steps) are cumulative. Evidence of an excessive profit margin is not sufficient in itself to prove an abuse. The EU competition authorities employ a cost– price approach in order to determine the excessive character of a profit margin. With regard to the measurement of the 'excessive' nature of the prices, a possible option is to determine an adequate cost measure to measure profit (adopt a cost-plus approach), compare that to the price and then to assess the excessiveness of the profit margin, the last operation involving the definition of some benchmarks. Some profit margin would also be entirely justified in dynamic industries or industries with network effects.

As to the adequate benchmark prices that would define the 'unfair' character of the prices charged, a comparison with the prices charged by competitors might be a possible option (although one should be cautious, as price differences may indicate quality differences). In *United Brands* the Court 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.'[105] Other options include the comparison with the price of the product over

other same or similar products or services; (ii) comparison with other geographic markets; (iii) comparison with historical prices: Article 14 of the Interim Provisions on Prohibiting Abuse of Dominant Market Positions.

In **South Africa**, the regime for excessive pricing adapted the test of EU Competition Law in United Brands. However following the decision of the Competition Appeal Court in *Sasol Chemical Industries Ltd v The Competition Commission* 2015(5)SA471(CAC) where the Commission failed to prove its case based upon the United Brands type test the law was amended in 2018 .While it remains a case of abuse of dominance for a dominant firm to charge an excessive price for a good or service , the amendment has changed the test as is shown by way of the following change to s8 of the Act : If there is a prima facie case of abuse of dominance because the dominant firm charged an excessive price, the dominant firm must show that the price was reasonable.

> 'Any person determining whether a price is an excessive price must determine if that price is higher than a competitive price and whether such difference is unreasonable, determined by taking into account all relevant factors, which may include—(a)the respondent's price-cost margin, internal rate of return, return on capital invested or profit history;(b)the respondent's prices for the goods or services—(i) in markets in which there are competing products;(ii) to customers in other geographic markets;(iii) for similar products in other markets; and(iv) historically;(c)relevant comparator firm's prices and level of profits for the goods or services in a competitive market for those goods or services;(d)the length of time the prices have been charged at that level;(e)the structural characteristics of the relevant market, including the extent of the respondent's market share, the degree of contestability of the market, barriers to entry and past or current advantage that is not due to the respondent's own commercial efficiency or investment, such as direct or indirect state support for a firm or firms in the market'.

[102] Case C-27/76 *United Brands v Commission* [1978] ECR 207.
[103] Ibid., 251.
[104] Ibid., 252.
[105] Ibid., para 253.

different geographic markets.[106] Hence, according to EU competition law, a price can be unlawfully excessive where 'it ha[d] no reasonable relation to the economic value of the product supplied' and assessed the prices using the following test: (1) whether the difference between the costs and the price was excessive ('excessiveness limb'); and (2) whether the price was either unfair (a) in itself or (b) when compared to the price of competing products ('unfairness limb')[107]. From an economic perspective, excessive extraction should be of concern only If it results from some form of market failure, such as lack of competition or other barriers that make it difficult for consumers to switch to competitors that would extract less data. However, the concept of fairness used provides some leeway to the enforcer to determine broader standards.

Applying this test to the issue of excessive data extraction, Robertson argues that 'one may in a first step need to look at the amount of personalized data gathered through third-party tracking (the price payed by the user), and what the user receives in return (the product's cost to the service provider and its economic value)', thus assessing 'whether there is a reasonable relation between the amount of data collection that the tracker can or will carry out and the economic value of the digital service the users receive'[108].

It is important in this context to determine, as a first step, the 'economic value' of the product, that is, the objective value that consumers would apply to the specific product in the counterfactual of a 'normal and sufficiently effective' competitive market (the benchmark price) and then determine if the difference between the price and cost in the factual compared to the counterfactual is excessive, the evaluation of costs most often deriving from a cost plus formula. This will involve the determination of which costs are relevant for pricing. Barriers to entry, such as network effects, may also be considered in the overall assessment of the likelihood that the levels of data extraction may be, or not, at a competitive level, thus determining the nature of the counterfactual.

Economic value cannot be determined in a similar way as in the context of the tangible economy, that is, simply on the basis of the various components of production costs (fixed, variable and sunk) plus a reasonable return on the costs the undertaking incurred with respect of the relevant product.[109] It is also important to compare with the level of extraction of data practised by platforms in more competitive markets, or the same platform over time, or across different customer segments, on a 'consistent basis' and employing 'objective, appropriate and verifiable criteria.'[110] In any case an overall assessment should each time be required.

---

[106] Ibid., para 239; Case C-395/87 *Ministère Public v Tournier* [1989] ECR 2521; Case C-110/88 *Lucazeau v SACEM* [1989] ECR 2811, the last two cases on the level of royalties charged by the French collecting society SACEM for playing recorded music in discotheques (acknowledging that important price differentials between Member States could indicate an abuse, unless the 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).

[107] See also, *Flynn Pharma Limited*, [2018] CAT 11

[108] V.H.S.E. Robertson, Excessive Data Collection: Privacy Considerations and Abuse of Dominance in the Era of Big Data (June 24, 2019), available at SSRN: https://ssrn.com/abstract=3408971 ,

[109] Other ways to determine this value relate to a comparison with other, more competitive markets, where no such conduct took place.

[110] Case C-177/16, Autortiesību un komunicēšanās konsultāciju aģentūra / Latvijas Autoru apvienība v Konkurences padome, ECLI:EU:C:2017:689, paras 41 & 51.

With regard to the cost-plus approach, as the digital service provided relates to the entertainment/content or convenience to the user (e.g. social media, the search engine), the cost should be related to the production of such services or convenience. However, a lot of the 'free' content available on some digital platforms is mainly produced and uploaded by the users themselves. The users also contribute to the attractiveness of the search engine by providing their data and thus enabling a better training for the platform's algorithms, thus enhancing its analytic skills through learning-by-doing. Hence, the first step of the analysis should involve some form of evaluation of the operational costs of the platforms linked to the provision of the digital service, and eventually any costs involved in the creation of content for some platforms, such as production costs (e.g. Netflix), payment to content contributors (e.g. You Tube) etc. Platforms may also argue that the data harvesting enables them to offer users targeted advertising, which should be considered as welfare-enhancing and thus forming part of the 'digital service' offered by the platform, as it constitutes an improvement in terms of time saved and search costs in comparison to the situation of across-the board advertising.[111] However, the welfare effects of targeted advertising are ambiguous and largely depend on the specific types of personal information made available through the targeting process.[112] The allocation of the benefits between the advertisers, the intermediary and consumers also varies and requires a case-by-case assessment. If targeted advertising constitutes adds a welfare gain to the user, then any cost involved in the provision of such digital service (for instance marketing costs) should form part of the assessment of the value of the economic value. In any case the simple fact that an undertaking earns above normal returns by harvesting more data does not prove the excessiveness of the data extraction.

As a second step in the analysis, one may determine if the price paid by the consumer has 'no reasonable relationship' with the value of the product. This looks to non-cost related factors, eventually also related to the demand side, such as network effects. As the (aggregate) demand curve indicates the maximum amount that potential customers would be willing to pay for each unit of a good, one may derive the customers' marginal economic valuations for each unit

One of the issues that may come up in the context of excessive data extraction cases is that the 'price' paid by the users takes the form either of data, which they agree to divulge to the platform and to third party trackers sometimes without knowing the real extent, or their attention/time. Users may also pay a 'price' to get access to the service. There are various models of monetisation of digital platforms, such as providing access for free while milking the 'money market', through subscriptions, offering a free and paid (premium) version (fermium), or an add-supported freemium.

Then comes the second step, which is to determine the unfair character of the amount of data harvested, either 'in itself or when compared to competing products.' As the UK CAT held in *Pfizer & Flynn Pharma*, excessiveness should not be assessed by reference to the theoretical concept of 'idealized or perfect competition' but the 'real world (where normal,

[111] C. Tucker, The Economics of Advertising and Privacy, (2012) 30(3) International Journal of Industrial Organization 326.

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

effective competition is the most that should be expected).'[113] Unfairness should also rely on a comparison with the level of data extraction in other comparable markets, and assess of the differential between economic value and 'price' is 'sufficiently significant and persistent to be excessive', as well as the evolution of this extraction of data over time, of course giving appropriate consideration to any objective justification advanced by the dominant undertaking.[114]

3.2.2. Personalised pricing

The practice of *behavioural pricing* or *personalised price discrimination*, which comes tantamount to first degree price discrimination (or person-specific pricing), is now possible in view of Big Data and algorithmic pricing as practiced in online commerce, as sellers charge different prices depending upon a buyers' search history, or "digital shadow"[115]. Firms may actively manipulate the choice of consumers.[116] Recent calls for intervention against "behavioural pricing" (or personalised price discrimination),[117] which may be considered as a form of algorithmic discrimination, illustrate the broader societal concerns (if not only economic) that are raised with regard to the perceived manipulation of consumers by companies, something as old as advertising exists.[118] In the era of "machine learning" and artificial intelligence-assisted pricing the risks of "digital" consumer manipulation may admittedly increase at an industrial scale.[119] Digital markets exacerbate the above risks, in view of the possibilities they offer of "a vast psychological audit, discovering and representing the

[113] *Flynn Pharma Ltd and Flynn Pharma (Holdings) Ltd v Competition and Markets Authority*, [2018] CAT 11.
[114] Ibid., para 443.
[115] M. Gal, 'Algorithmic-facilitated Coordination', DAF/COMP/WD(2017) 26 (noting that " (a)s 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").
[116] See, J D. Hanson & D A. Kysar, Taking Behavioralism Seriously: The Problem of Market Manipulation, (1999) 74 New York University Law Review 630. For the first study in EU competition law raising this problem, see N. Economides & I Lianos, The Elusive Antitrust Standard on Bundling in Europe and in the United States in the Aftermath of the Microsoft cases, (2009) 76 Antitrust Law Journal 483, 542.
[117] See, Autorité de la Concurrence & Bundeskartellamt, Competition Law and Big Data (May 10th, 2016), 21-22, noting 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, see German Federal Supreme Court (BGH), „Entega II", KZR 5/10, judgment of 07.12.2010. For a discussion of "personalised pricing" see, P Coen & N Timan, 'The Economics of Online Personalised Pricing' (Office of Fair Trading 2013); Oxera, 'Behavioural Economics and Its Impact on Competition Policy' (Oxera 2013) ; T.J. Richards et al, Personalized Pricing and Price Fairness, (2015), available at https://courses.cit.cornell.edu/jl2545/papers/personalized_Pricing_IJIO.pdf ; A Ezrachi & M Stucke, 'The Rise of Behavioural Discrimination' [2016] 37 ECLR 484; A Ezrachi & M Stucke, Virtual Competition (Harvard University Press 2016), Chapter 11 (distinguishing "near perfect" discrimination, involving the categorisation of consumers through the harvesting of personal information collected with the help of Big Data and self-learning algorithms, from "behavioural" discrimination, which is led with the aim to trigger consumer biases and increase consumption).; M Bourreau et al., Big Data and Competition Policy: Market Power, personalised pricing and advertising, CERRE Project Report (February 2017).
[118] See, I Lianos, 'Brands, Product Differentiation and EU Competition Law' in D. Desai, I. Lianos & S. Weber Waller (eds.), Brands, Competition Law and IP (Cambridge University Press, 2015), (discussing the 'persuasive view" of advertising in economic literature).
[119] R Calo, 'Digital Market Manipulation', (2014) 82 George Washington Law Review 995.

desires of society" [120] and of each individual separately, offering sophisticated evaluation methods that are closely linked to the direct observation of consumer preferences, but also more broadly of a whole range of preferences expressed in social, and private life, through the means of sociometric analysis[121]. Big data enable us to observe, allegedly more accurately, the inner mental states of people and potentially influence the way these form their core preferences. Such manipulative potential and of course the possibility that this may occur at a larger scale, in view of the possibilities offered by algorithms, data analysis and artificial intelligence, is clearly motivating public authorities to action.

This may later feed in the companies' commercial strategies that may, for instance, develop personalised pricing strategies, which may be considered a form of price discrimination. Price discrimination may be of different types:

- *First degree price discrimination*: it enables the producer to set individualized prices for each customer, relying on its knowledge of *individual* preferences
- *Second degree price discrimination*: The producer doesn't know the individual preferences and proposes a menu of options to consumers, letting the consumers choose their preferred one.
- *Third degree price discrimination*: The producer doesn't know the individual preferences, but charges different prices to groups of consumers with different characteristics.

There is price discrimination when two transactions of the same good occur at different prices despite having the same cost. Successful, from the company's perspective price discrimination (that is one that cannot be defeated by consumers switching to other producers) requires some conditions, including (i) market power, (ii) the ability to distinguish customers, (iii) the ability to prevent resale. Personalised pricing improves the ability to distinguish customers and may lead to first degree price discrimination, as well as third degree price discrimination, when it is possible for the firms to apply group pricing, discriminating between groups of consumers. Subjecting to price discrimination final users may enable the producer to capture the entire consumer surplus, generate unequal treatment of various individual consumers or groups of consumers, and affect competition with other producers (not necessarily of the same relevant market), in the sense that by enabling the producer to charge a specific consumer as high as his willingness to pay, reduces the available income of the consumer to make other purchases. Different producers compete for the limited resources/budget of a consumer or a group of consumers. As a result consumer welfare suffers, in comparison to the counterfactual, which is here perfect competition and uniform pricing that is marginal cost pricing (might in digital markets may be close to zero).

Personalised pricing or "price targeting" has been observed in various markets.[122] To the extent that this manipulation may result in welfare losses for individuals, or group of consumers, in the sense that the specific individual, or the specific group of consumers, could find its/their situation worse off, in comparison to a counterfactual where no such digital

[120] W. Davies, The Happiness Industry: How the Government & Big Business Sold Us Wellbeing (Verso, 2015).
[121] Ibid.
[122] See the analysis and examples provided in M Bourreau et al., Big Data and Competition Policy: Market Power, personalised pricing and advertising, CERRE Project Report (February 2017), 40-41 and the empirical studies they refer to.

manipulation would have taken place, it can be argued that these deviations from the counterfactual situation need to be corrected through State intervention, eventually by competition law enforcement. But this is a matter for debate. One may argue that personalised pricing should not be considered as a form of 'manipulation', but as a technological opportunity to charge each consumer as much as her/his willingness to pay is. This may, for instance, enable some consumers that would not have been able to purchase the specific product, if a uniform price would have been implemented and would have been higher than their willingness, to afford the product. 'Personalised pricing' may therefore have ambiguous welfare effects, depending on the market structure and the trade of between the market 'appropriation' effect to consumers with high willingness to pay versus the 'market expansion' effect to consumers with a low willingness to pay.[123] In *Asnef-Equifax*, when examining the possible efficiency gains brought by a restrictive to competition information exchange, 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'[124]. Hence, it seems that this assessment should be done at a general level, the representative consumer of the specific relevant market.

One may also argue that EU competition law's focus on distributive justice, in particular its emphasis on the position of 'consumers', who should not be worse off following the specific conduct, may justify competition law intervention if the additional benefits from personalised pricing are not passed on to them, 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 personalised pricing is not transparent and thus consumers are not informed, or the need to limit an extensive use by the firms practising algorithmic discrimination of consumers' sensitive personal data, in view of the purpose limitation and data minimisation requirements in the Data Protection regulation.[125] These practices may also raise more conventional competition law concerns, as they discourage consumer search by making it harder 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 finish paying higher prices.[126]

There are different ways to deal with personalised pricing, from a competition law perspective. In the EU, it is possible that such practices may be qualified as a form of price discrimination under Article 102(c).[127] Article 101(1)(d) TFEU also prohibits agreements that

[123] For a discussion, see OFT1488, The economics of online personalised pricing (May 2013), available at http://webarchive.nationalarchives.gov.uk/20140402142426/http:/www.oft.gov.uk/shared_oft/research/oft1488.pdf ; M Bourreau et al., Big Data and Competition Policy: Market Power, personalised pricing and advertising, CERRE Project Report (February 2017), 43-45.

[124] 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, para. 70 (emphasis added).

[125] Art. 5(1) of Regulation **(**EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation - GDPR), [2016] L 119/1. See also Art. 9(1) GDPR and Section 2 of the Data Protection Act 1998 which require the data controller when processing personal data to obtain a specific and explicit consent to process these categories of data.

[126] M Armstrong & J Zhou, 'Search Deterrence' (2016) 83 Review of Economic Studies 26

[127] See, Autorité de la Concurrence & Bundeskartellamt, Competition Law and Big Data (May 10th, 2016), 21-22, noting that although the application of EU competition law to these practices may be debated, in Germany, the

"apply dissimilar conditions to equivalent transactions with other trading parties, thereby placing them at a competitive disadvantage." Article 102(c) utilizes almost identical language to inhibit dominant undertakings from engaging in price discrimination. EU competition authorities have focused price discrimination enforcement on dominant undertakings. Among the conditions for the application of this provision, there is the requirement that the "other trading partners" are placed at a "competitive disadvantage", which may suggest that this provision may not apply to discrimination on price or other parameters of competition against final consumers. However, this language has not impeded the Commission to apply Article 102(c) to final consumers in *Deutsche Post*, in particular consumers of postal services, which due to the behaviour of Deutsche Post were affected negatively by having to pay prices for these services which were "higher than those charged to other senders and by having their mailings delayed significantly" 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 be applied in situations where a dominant undertakings behaviour causes damage directly to consumers."[128]

Also note that the case law does not require evidence of a competitive disadvantage, which in some cases has been presumed.

Alternatively, personalised pricing may be attacked through Article 102(a) if it can be qualified as 'directly or indirectly imposing unfair purchase or selling prices or other unfair trading conditions,' for instance because it has led to the imposition of a higher price (or lower quality) than what would have been the case but for the specific digital manipulation and enables the producer to capture the entire consumer surplus. Of course, should this route be followed, it would be important to design a test with more specific conditions than just the fact that there is no reasonable relation between the price charged to the consumer and the "economic value" of the product supplied, as personalised pricing aims precisely to set the price at the exact level the specific consumer thinks is the 'economic value' of the product (subjective perception of value that corresponds to the subjective willingness to pay of this specific consumer), which from an economic efficiency perspective should not be problematic. However, one may argue that the principle of 'open market economy' would require that economic value should be set in the context of a competitive process taking place on a market, where various actors, consumers and suppliers interact, in view of the fact that 'competition is, by its very essence, determined by price.'[129] Hence, charging a consumer a personalised price that would correspond to her/his willingness to pay, without him being aware of this and without enabling the specific consumer to benefit from the competitive process taking place at the 'open market' and the source of information this may provide so as to enable informed comparison with regard to the situation of other consumers may contravene to 'the principle of

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, see German Federal Supreme Court (BGH), „Entega II", KZR 5/10, judgment of 07.12.2010.

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

[129] 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, para.18.

an open market economy with free competition.'[130] This is particularly important as one may argue that consumers value the competitive process as such, and not just the fact that the price of a product is within the range of their willingness to pay, which is also something that cannot be set in advance, but essentially cultivated in the context of a market involving continuous interactions between buyers and sellers. That said, it is important to explore if competition law is the best legal instrument to deal with welfare-reducing targeted pricing, or if other alternatives, such as consumer protection law, data protection and privacy rules, anti-discrimination law, unfair commercial practices law, free movement law, regulation, may prove to be more appropriate, following a detailed comparative institutional analysis.[131]

3.2.3. Unfair commercial practices and trading conditions

The exploitation of trading partners may not only take the form of higher prices. In some competition law regimes, the imposition of 'unfair trading conditions' (UTC) or 'unfair commercial practices' (UCP) may also constitute an abuse of a dominant position,[132] and this even if other areas of law, such as unfair competition or contract law may also apply in this occasion. The concepts of UTC and UCP are quite broad, and fuzzy, thus offering an important policy discretion to competition authorities and a high margin of interpretation to the courts to frame the scope of this legal category in the way they find appropriate. In some well-established case law, the CJEU considered that contractual provisions that have an 'inequitable nature' may constitute an abuse, 'bearing in mind both the intrinsic individual effect of those clauses and their effect when combined.'[133] Similarly, the CJEU found abusive contractual clauses 'making access to [a distribution] network conditional upon the firms accepting unfair terms in the distribution agreement,' these constituting UTC.[134] These practices need not derive directly from the contract but may also consist in measures unilaterally adopted by the dominant undertaking, not always in the context of a pre-existing contractual relation. National

[130] This principle is mentioned in Articles 119, 120 and 127 TFEU.

[131] See, M Bourreau et al., Big Data and Competition Policy: Market Power, personalised pricing and advertising, CERRE Project Report (February 2017), 45-47, noting restrictions on personalised pricing from data protection rules (the need to have the explicit consent of the data subject involved), consumer protection rules (disclosure to consumers about the prices and how they are calculated), unfair commercial practices (prohibiting in certain circumstances consumer profiling and considering this as a misleading commercial practice), free movement law (the Services' directive prohibitions to 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.

[132] See, for instance, Article 102(a) providing as an example of abuse 'directly or indirectly imposing […] unfair trading conditions.'

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

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

competition authorities have been quite active on this front, even for non-dominant undertakings.[135] Although this case law on UTC and UPC focuses on practices affecting other undertakings (B2B), there is nothing that would impede these from also applying with regard to UCP and UTC affecting final consumers (B2C), as there is not distinction between situations in which the dominant undertaking is in competition, or not, with its trading partner downstream or upstream. Hence, the provisions prohibiting an abuse of a dominant position could also cover conduct imposing unfair conditions to final consumers that would lead to a reduction of the quality of the services provided and other exploitative effects, such as the extraction of personal data without the user's consent.

This raises, however, the question of what may constitute UCP or UTC under EU competition law, and 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. Some recent soft law and preparatory documents relating to the adoption of the Directive concerning unfair business-to-consumer commercial practices,[136] the Directive on unfair trading practices in business-to-business relationships in the food supply chain,[137] or the recent EU regulation on platform to business regulation,[138] may provide a source of inspiration for this case law to develop further.

One needs of course to distinguish carefully between the interpretation of Article 102 TFEU of the Treaty and the emergence of some EU unfair competition law. The fact that a practice constitutes, or not, an 'unfair' commercial practice under the EU Unfair Trading Practices in the food sector or the EU Regulation on fairness in the context of intermediation platforms, should not have an immediate bearing on the qualification of such practice as an UCP or UTC prohibited by Article 102(a) TFEU. However, it does constitute a factual element that needs to be taken into account when interpreting the meaning that the prohibition of 102(a) on unfair trading conditions. Some common elements seem to define the concept of UPC and UTC in this context. The Commission has 'broadly' defined UTC as 'practices that grossly deviate from good commercial conduct, are contrary to good faith and fair dealing and are unilaterally

[135] A. Renda et al., Study on the Legal Framework Covering Business-to-Business Unfair Trading Practices in the Retail Supply Chain – Final Report (February 26, 2014), available at https://publications.europa.eu/en/publication-detail/-/publication/c82dc8c6-ec15-11e5-8a81-01aa75ed71a1/language-en .

[136] 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, [2005] OJ L 149/22.

[137] European Commission, 'Green Paper on Unfair Trading Practices in the Business-to-Business Food and Non-food Supply Chain in Europe' COM(2013) 37 final ; European Commission, 'Communication, Tackling unfair trading practices in the business-to-business food supply chain' COM(2014) 472 final ; European Commission, 'Staff Working Document, Impact Assessment, Initiative to improve the food supply chain (unfair trading practices), Accompanying the document, Proposal for a Directive on unfair trading practices in business-to-business relationships in the food supply chain' SWD(2018) 92 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.

[138] European Commission, 'Staff Working Document, Impact Assessment, Annexes, Accompanying the document, Proposal for a Regulation on promoting fairness and transparency for business users of online intermediation services' (2018) 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; 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.

imposed by one trading partner on another.'[139] In defining the problem requiring intervention, the Commission also insisted on the 'transfer of excessive risk and costs to weaker parties' and a 'diminished part of added value' for the 'weaker' parties as some of the implications of UTC in the presence of an unbalance of bargaining power.[140] The overall concept thus refers to practices of value capture that lead to an 'unfair' division of surplus between the actors involved. However, the way the concepts of UPC or UTC have so far been conceptualized in these texts is intrinsically linked to the B2B dimension of vertical competition these rules aim to regulate, as it assumes that the 'weaker' actor is an undertaking taking risks, rather than a final consumer. Hence, such conceptualisations may provide useful insights but certainly do not exhaust the conceptual potential of the UTC and UPC.

A recent case brought by the German competition authority against Facebook (*Bundeskartellamt, BKA*) raises interesting issues as 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.[141] Facebook collected the data of its users by merging the various sources of personal data generated by the use of Facebook-owned services, such as WhatsApp or Instagram, or by the use of third party websites and apps, which 'embedded' Facebook products through the 'like' button and the use of Facebook analytics. The BKA differentiated between user data that were generated through the use of Facebook, and user data obtained from third party sources, either controlled by the Facebook corporate group, such as Whatsapp, Oculus, Masquerade, or through the use of Facebook programming interfaces in websites or mobile apps in third party providers websites (via the Facebook developer platform and Facebook Business Tools), these being data not generated by the use of Facebook's social network and for which Facebook has not received the user's consent.

The BKA raised concerns with regard to the possible existence of an abuse of a dominant position as Facebook made the use of its service conditional upon the user granting the company extensive permission to use his or her personal data, even those generated off-Facebook use, in particular through the possibility of Facebook to gather user-related and device-related data gathered and saved during ether the use of the Facebook-owned third parties or through the Facebook Business Tools in third-party websites. Users were, therefore, no longer able to control how their personal data was used. The decision focused on the infringement of German competition law, in particular Section 19(1) 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 which data and from which sources were being merged to develop a detailed profile of their identities and their online activities.

In determining the existence of abuse, the BKA delved into the analysis of Facebook's terms of service and data policy. It examined whether Facebook's data processing terms were admissible in view of the principles of the harmonised European data protection rules (EU

[139] European Commission, 'Communication, Tackling unfair trading practices in the business-to-business food supply chain' COM(2014) 472 final, 2.

[140] European Commission, 'Staff Working Document, Impact Assessment, Initiative to improve the food supply chain (unfair trading practices), Accompanying the document, Proposal for a Directive on unfair trading practices in business-to-business relationships in the food supply chain' SWD(2018) 92 final, 11.

[141] Bundeskartellamt, Facebook decision (2019), https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Entscheidungen/Missbrauchsaufsicht/2019/B6-22-16.pdf?__blob=publicationFile&v=5 (hereinafter BKA, Facebook).

General Data Protection Regulation). In doing so BKA indicated that a violation of EU data protection law could give rise to an abuse of a dominant position. This approach is consistent with that followed by the other German competition authority, the Monopolkommission, in proceedings pending before it. According to the Monopolkommission, an infringement of statutory provisions other than those relating to competition becomes a competition law problem if the infringement is either the result of a dominant position or it confers a competitive advantage which allows the dominant undertaking to distort competition.[142] 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 prohibiting conduct of dominant undertakings (§ 19 GWB) could apply.

Facebook challenged these conclusions, arguing that there was no causal link between the alleged abusive conduct by Facebook and a dominant position on the market, as a number of other non-dominant companies were employing the same practices[143]. The BKA rejected this argument noting that these terms and conditions and data policy infringed Section 19 GWB, 'because, as a manifestation of market power, these terms violate the principles of the GDPR'[144]. It seems therefore to establish a direct link between an infringement of competition law and an infringement of the principles of data protection. The BKA referred to past case law of the German Federal Court of Justice which 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.'[145] The BKA inferred from this case law the general principle that 'an abusive practice can also be found based on the general clause of Section 19(1) GWB prohibiting an abuse of a dominant position by one or several undertakings, e.g. where general business terms are used 'that are inadmissible under the legal principles of Sections 307 and subsequent provisions of the German Civil Code (BGB),[146] and in particular where these practices also represent a manifestation of market power or superior market power.'[147] This allows for a quite broad interpretation of the scope of abusive business terms (and potentially of their EU law equivalents UTP or UTC), in particular as the BKA also insisted that determining whether the business terms are abusive necessitates 'an extensive balancing of interests... which should also take into account constitutionally protected rights.'[148] Hence,

[142] Monopolkommission, 'Sondergutachten 68: Wettbewerbspolitik: Herausforderung digitale Märkte' (June 2015) Tz. 517. <https://www.monopolkommission.de/de/gutachten/sondergutachten/sondergutachten-68.html>.
[143] BKA, Facebook, para.156.
[144] Ibid., para 523.
[145] Ibid., para. 526.
[146] According to Section 307 BGB,
'(1) Provisions in standard business terms are ineffective if, contrary to the requirement of good faith, they unreasonably disadvantage the other party to the contract with the user. An unreasonable disadvantage may also arise from the provision not being clear and comprehensible.
(2) An unreasonable disadvantage is, in case of doubt, to be assumed to exist if a provision
1. is not compatible with essential principles of the statutory provision from which it deviates, or
2. limits essential rights or duties inherent in the nature of the contract to such an extent that attainment of the purpose of the contract is jeopardised.'
[147] Ibid., para. 527.
[148] Ibid.

Section 19 GWB 'should be applied in cases where one contractual party is so powerful that it would be practically able to dictate contractual terms, thus eliminating the other party's contractual autonomy.'[149]

In interpreting the prohibition principle in Section 19(1) the BKA was inspired by the content of some of the examples of abusive conduct mentioned in Section 19(2) GWB, and in particular 19(2)1 and 19(2)2. One may determine the abusive nature of the trading conditions and commercial practices from a comparison of business terms 'which differ from those which would very likely arise if effective competition existed', in particular by taking into account the conduct of undertakings in comparable markets where effective competition exists, according to Section 19(2)2. However, this is not the only way to determine the abusive and unfair nature of business terms and trading conditions, the BKA referring to 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.'[150] The aim is to preserve the 'constitutionally protected right to self-determination in business affairs (commercial freedom) because the other part is able to *unilaterally* determine the terms of the contract.'[151] This unilateralism in the determination of the conditions of the contract breaks with the usual assumption in contract law about the existence of a mutually beneficial agreement based on consent and a meeting of minds. It hints to the fact that the transaction in question may be better described by the concept of 'uncontract'.[152]

This legal construction enables the BKA to integrate in the context of the enforcement Section 19 GWB any restriction to the duty of 'appropriateness' included, more broadly, in the 'constitutional principles' involved in the protection of the right to informational self-determination and the fundamental right to data protection' and the principles of relevant legal provisions, such as the rules concerning the appropriateness of data use, included in the data protection legislation (GDPR).[153] This quite broad construction of abusive business terms by the BKA seems limited by the requirement that 'a sufficient degree of market power is involved'[154] and by the fact that data protection law follows similar goals to the prohibition of abusive business terms in competition law, in particular in its role as a 'special economic law' which aims to achieve 'a balancing of interests between data processors and the consumers' and 'counter power asymmetries between organisations and individuals'[155]. The BKA also takes a broad view of the concept of abusive business terms as it includes data processing terms and data policies, considered as part of the terms of service, in view of the regulatory character

[149] Ibid.
[150] Ibid., para. 528.
[151] Ibid.
[152] See, S. Zuboff, *The Age of Surveillance Capitalism*, (Public Affairs, 2019), 208 et seqq. As she describes it:
> 'The uncontract is not a space of contractual relations but rather a unilateral execution that makes those relations unnecessary. The uncontract desocializes the contract, manufacturing certainty through the substitution of automated procedures for promises, dialogue, shared meaning, problem solving, dispute resolution, and trust: the expressions of solidarity and human agency that have been gradually institutionalized in the notion of "contract" over the course of millennia. The uncontract bypasses all that social work in favor of compulsion, and it does so for the sake of more-lucrative prediction products that approximate observation and therefore guarantee outcomes'.

[153] BKA, Facebook, para. 529.
[154] Ibid., para. 528.
[155] Ibid., para. 530.

they have from the perspective of users.[156] Hence the BKA arrives to the conclusion that 'abusive business terms pursuant to Section 19(1) GWB could also be examined… with respect to a violation of Section 307 BGB which in turn refers to the mandatory principles of the GDPR.' This raises, more broadly, the question of the relationship between competition law and data protection law.

The BKA seems to proceed to a reasoning in two steps.

First, it acknowledges that Facebook's terms and conditions and data policies constitute a violation of GDPR data protection values.[157] It proceeds to a very detailed analysis of the GDPR framework and the possibilities of justification that Facebook could have put forward as part of the data protection law assessment. The BKA takes issue with Facebook's data processing, in particular profiling, in particular the fact that information collected in Facebook-owned separate websites are used for profiling purposes on Facebook, and rejects the argument put forward by Facebook which claimed that the fact that these companies form part of its corporate group would have enabled it to use this data without infringing the GDPR. The BKA delves into the analysis of the concept of 'group of undertakings' in Article 4(9) of the GDPR and concludes that contrary to Facebook's view, no group privilege may be derived. Interestingly, in interpreting the GDPR the BKA notes that 'intra-group transactions are not generally exempt from abuse control if they have restrictive effects on competition', giving the example of bundling products within the same group, that would have raised, if accepted, the risks of transfer of market power or exploitation of the opposite side of the market[158].

This reference to competition law aims to establish some form of conceptual coherence between these two separate regimes, although the BKA is careful to note that this is a response to Facebook's argument that competition law recognizes group privileges. Following a quite thorough analysis, the BKA also finds no justification of such practices under Articles 6 and 9 of the GDPR. In particular, the BKA notes the absence of voluntary consent by the users for this data aggregation, in view of the take-it-or-leave it and conditional nature of the exchange and the 'clear imbalance' between the data comptroller and the data subject in this case, as Facebook disposes of a dominant, almost quasi-monopolistic, position on the market[159]. Indeed, 'it cannot be assumed that individuals give their consent voluntarily since users are forced to consent to data processing terms when they sign up for a service provided by a company that has a dominant position in the market.'[160] 'Free choice' within the meaning of data protection law cannot be assumed in the presence of such 'clear imbalance.' Finally, the BKA notes that the need to process data collected from other Facebook-owned services or third parties is not necessary for the performance of the contract with the Facebook user, in particular as the contents of the contract are unilaterally imposed on the data subject by the data comptroller.

The BKA observed that Facebook has a 'special responsibility' when considering the necessity of the data processing conditions unilaterally imposed, in view of the difficulty of users to evade the terms of service of Facebook in view of its dominance and hence one needs

[156] Ibid., para. 534.
[157] Ibid., paras 573 et seq.
[158] Ibid., para. 613.
[159] Ibid., paras 645 & 646
[160] Ibid., para. 643.

to examine thoroughly the existence of voluntary consent for the processing of data. It also rejected Facebook's argument that the data processing was necessary for contractual purposes, as it enabled a more personalized user experience and the need to improve the quality of the service to the users. The BKA noted that '(t)his 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 that the BKA categorically rejected[161]. Indeed, the BKA stipulated with regard to the collection of data of Facebook use that this was not necessary as Facebook could have achieved a high degree for personalization with the data generate from the Facebook website itself[162]. This is particularly interesting as it may constitute an argument that may also be relevant in the context of excessive data extraction claims and would neutralize the argument often put forward 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 also doubt of the effectiveness of this argument in view of the fact that this increased personalization may lead to instances of future exploitation, and not just for enabling targeted advertising. As the BKA notes, '(a)nother particularly problematic aspect' of such data processing as the aggregation of data across Facebook-owned and third party websites enables 'active fingerprinting' and 'detailed profiling' of the users that 'leads to a massive additional invasion of privacy, since profiling 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.'[163]

It is remarkable that although the BKA made efforts to interpret the relevant provisions of the GDPR according to data protection law, it frequently made references 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 'consistency of the user experience' by noting that integrating services or functionalities, and share user data, 'is problematic under antitrust law' in view of the leveraging or maintenance of market power concerns that this may raise and the possibility to exclude other market players, create barriers to new entrants and enhance the lock-in effect by making switching providers more difficult.[164]

In exploring the compatibility of Facebook's practices to the GDPR, the BKA took into account the legitimate interests of the affected stakeholders, in particular third parties, such as advertisers that want to buy targeted advertising from Facebook, and Facebook users. Of particular interest is the fact that the German competition authority has also framed the issue as relating to the protection of the citizens' constitutionally protected rights to 'informational self-determination.' To do this, the BKA did not, as usually competition authorities do, rely only on the preferences of the users/consumers as these are revealed in the marketplace, but made reference to the interests of the users/citizens as these 'revealed' in constitutional principles. The authority considered the promotion of 'informational self-determination' a socially valuable aim, as it is constitutionally protected, and did so without relying on

[161] Ibid., para. 692.
[162] Ibid., para. 744
[163] Ibid., para 847.
[164] Ibid., paras 747-739.

consumers' preferences. According to the BKA, to the extent that the 'information sovereignty' of users is affected by continuous distortions by governments and businesses which are 'increasingly able to create detailed profiles predicting their behaviour (thereby exacerbating information imbalances and undermining personal autonomy) it is all the more important to ensure that the interests of individuals in the protection of their privacy and autonomy are safeguarded.'[165]

Interestingly, the authority could have also focused on the quality dimension of competition and its reduction by the 'loss of control' of the users as they were no longer able to control how their personal data were used. However, the BKA made no effort to build such a quality narrative, simply because it would have had to explain why the users had not switched to different social networks if 'informational self-determination' was a parameter of quality and variety competition. For this to happen, the price revealed preference (or a contingent valuation method) would have required some analysis of substitutability between social networks that respect informational self-determination and those, like Facebook, that violated this principle. In contrast, the evidence basis on which the BKA seems to have built its theory of harm relates more to the citizens' right to informational self-determination/privacy, as these are proclaimed and protected by the German constitution and data protection law.

The BKA balanced these rights of Facebook users for self-determination with the rights of Facebook for entrepreneurial freedom. In exercising the balancing the German authority noted that the legitimate interests of Facebook cannot outweigh those of the Facebook users, in particular as the data processing was not necessary, and in view of the broader harms and disadvantages that such processing 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 comptroller.[166] With regard to the last factor, the BKA took into account the fact that 'as a multinational company with a dominant position in the market, Facebook has the negotiating power to impose extensive data processing unilaterally on users', in view of its 'special bargaining power.'[167] This assessment of the position of Facebook was found relevant for performing the balancing of interests of the data subjects and data comptrollers and third parties according to data protection law. The BKA found relevant for this assessment the fact that Facebook unilaterally imposed these conditions on data processing to the users in its terms and conditions and data policies and that such policies present the 'risk of further strengthening Facebook's market power vis-à-vis-users by transferring this market power to other services', thus by the same 'strengthening the bargaining power and the possibility of imposing terms unilaterally.'[168]

These concerns are very well inspired by competition law theories of harm, such as leveraging and monopoly maintenance, now repurposed for the occasion as data protection theories of harm. Such harm may, according to the BKA, be even more important for users with some degree of vulnerability, such as adolescents.[169] This introduces a horizontal fairness dimension as it makes possible the distinction between different groups of users, according to

[165] Ibid., para. 760.
[166] Ibid., para. 767.
[167] Ibid., paras 783 & 785.
[168] Ibid., para 785.
[169] Ibid., para. 786.

the degree of their vulnerability vis-à-vis the data comptroller. This detailed interests balancing was performed for both the conduct involving the processing of data harvested by Facebook-owned services, as well as those collected through the Facebook Business Tools, again arriving to a similar conclusion that the rights of the users outweigh those of Facebook and other third parties.[170] By finding that the GDPR-based justifications for Facebook's conduct did not apply, in view 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 as to the existence of an infringement of the principles of the GDPR. This however did not automatically result to a competition law infringement, the BKA proceeding during the second step of the analysis to the competition assessment of this conduct.

Second, the BKA analysed how the infringement of data protection may be abusive *within the meaning of the competition law provisions*, in particular Section 19(1) GWB (the BKA conveniently choosing to focus on national competition law, for which it has some discretion, in particular in view of Article 3(2) of Regulation 1/2003)[171]. The analysis here is structured in two sub-steps, the BKA first observing that there is some causal link between Facebook's market power and the abusive (according to data protection law) data processing conditions it imposes to its users, and then proceeding to a balancing of interests under antitrust law. With regard to the first step, the BKA adopted a rather flexible concept of causal link, not requiring evidence that the dominant position/market power was a necessary prerequisite for the specific abuse, but rather a sufficient condition. 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.'[172] 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 a single, most important causal factor.[173] According to the BKA, 'there is a normative-causal connection in the vertical relationship with private users between the existence of a dominant position in the market and the violation of the relevant assessments under data protection law', bringing it to the conclusion that the violation of data protection requirements in this case 'is a manifestation of Facebook's market power.'[174]

Although this does not mean that this step of the antitrust analysis completely merges with the analysis under data protection law, at least at a conceptual level, in practice it becomes unclear how the two may refer to different issues. The BKA proceeds by integrating traditional competition law concerns over market power and the special responsibility of dominant firms in data protection law, putting some effort in advancing the conceptual consistency between these two regimes. Hence, it is now argued, 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

[170] Ibid., para. 836.
[171] Art. 3(2) of Regulation 1/2003, provides, *inter alia*, that 'Member States shall not under this Regulation be precluded from adopting and applying on their territory stricter national laws which prohibit or sanction unilateral conduct engaged in by undertakings'.
[172] BKA, Facebook, para. 873.
[173] Ibid., paras 873 & 875.
[174] Ibid., para. 879.

would need to be assessed differently' than undertakings with market power.[175] This brings the BKA to argue that data protection law takes into account the individual circumstances of the company, in particular its market dominance, in particular in the way it assesses the way the data was processed and possible justifications. It also enables it to reject the idea of accepting the data harvesting and processing allegedly violating data protection law as an 'established industrial standard' justifying Facebook's policies to the extent that smaller rivals proceed to similar practices. According to the BKA, accepting this 'could lead to the paradoxical outcome that smaller competitors… might be tempted to act in violation of data protection law under the "umbrella" of the dominant undertaking and the dominant undertaking could then refer to competitors' conduct to justify its own behaviour.'[176] For the reasons mentioned above, the BKA does not have issue with the fact that under its interpretation a dominant undertaking, such as Facebook, may be subject to stricter data protection requirements than non-dominant undertakings.

Notwithstanding these remarks about the existence of a normative causal link, the BKA also considered that there was a strict causality between the data policies found problematic and Facebook's dominant position as there was at least some 'correlation' of the violation of data protection law with market power.[177] The interpretation of the existence of a causal link becomes more apparent when the BKA examines the causal relationship between the unlawful data processing and Facebook's market dominance with regard to the possible harm to competitors. The BKA notes that in advertised-based platforms, there is a high incentive for the platform to adopt problematic data processing practices that give access to the users' data harvested from Facebook-owned services or third parties, as this helps the platform to make attractive offers to advertisers in the form of targeted advertising.[178] This risks however 'transferring market power' by making it more difficult for users, because of enhanced personalisation also in the context of these services, and the standardisation of product experience throughout Facebook-owned services to switch providers, thus reinforcing the network effects.[179] This may also increase barriers to entry for potential competitors in the market for social networks.

The second sub-step is the performance of a balancing of interests, this time under antitrust law, taking into account the objective of the German competition Act to promote free competition. However, strikingly, the BKA holds that if the terms of business violate data protection values *as a result of* market power, then the antitrust balancing does not have 'any independent significance' to the data protection balancing, thus effectively creating a presumption of anticompetitive effect if there is violation of data protection law in conjunction with evidence of some causal link, and this as indicated in the previous paragraph is determined rather liberally a simple correlation being found sufficient evidence, with the existence of market power. This does not impede the BKA to perform such balancing in this case, as a precaution, noting however that in this case this 'leads to the same outcome as the balancing

[175] Ibid., paras 879 & 882.
[176] Ibid., para. 884.
[177] Ibid., para. 880.
[178] Ibid., para. 887.
[179] Ibid.

of interests under data protection law.'[180] The necessity of independent additional balancing under antitrust law is according to the BKA challenged by the previous case law of the Federal Court of Justice, which emphasises 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 (antitrust) balancing of interests.'[181]

This rather blunt observation hints to the possibility that the BKA applies to conduct infringing data protection law a presumption of illegality under competition law, if there is some evidence of dominant position and of a loose causal connection between the conduct (data protection infringement) and the dominant position. This is explained from BKA's conception that 'the antitrust concept of the appropriateness of conditions relies on comparable concepts of appropriateness defined in other legal areas in similarly unbalanced negotiation situations such as legislation on general terms and conditions or data protection law', these appropriateness rules in these other legal areas being 'themselves the result of a balancing of interests with regard to the necessary reconciliation of interests in the negotiation of terms and conditions.'[182] The BKA also notes the similarity of the balancing factors, one of which is dominance, in both antitrust and data protection law, leading to the same outcome, which explains that the balancing of interests may be done 'simultaneously under antitrust and data protection law.'[183] Interestingly, the enforcement of Section 19(1) GWB is seen as aiming to bring about 'a balance of interests while taking the parties' constitutional rights into account.'[184] One could see in this reference to constitutional norms and principles, the development of meta-principles (operating across different areas of law) guaranteeing consistency of interpretation between antitrust and data protection law duties to dominant firms. This would involve the obligation to include assessments with regard to constitutional rights in assessments of interests under competition law, following the case law of the German Federal Court of Justice in *Pechstein.*[185] This is particularly significant, in particular in the presence of a dominant company unilaterally imposing problematic data policies and terms and conditions because it is 'not subject to sufficient competitive control,'[186] even more so 'if a monopoly or quasi-monopoly exists.'[187] The BKA observes that this makes it possible in the specific case of Facebook 'to determine the abuse directly by comprehensively balancing interests, taking the constitutional rights of the contracting parties into account with regard to the exclusion of voluntary self-determination as a result of market dominance.'[188] Essentially, this makes it possible to refer 'to the assessments under data protection law for the balancing of interests under antitrust law', to the extent that there is already 'a statutory decision on the balancing of fundamental rights' under the GDPR (Article 6(1), this 'technical substantiation'

[180] Ibid., para. 889.
[181] Ibid., para. 891.
[182] Ibid., para. 892.
[183] Ibid., para. 894.
[184] Ibid., para. 895.
[185] Ibid., para. 900, citing Federal Court of Justice, judgment of 7 June 2016, KZR 6/15 – Pechstein, para. 55 (juris).
[186] Ibid., para. 897.
[187] Ibid., para. 895.
[188] Ibid., para. 900

also applying to the antitrust perspective. For the BKA this 'unifies the balancing framework.'[189]

The BKA nevertheless makes some effort to connect the violation of data protection norms to some competition law theory of harm, hence the emphasis put on the reduction of consumer choice that an unlimited data processing from the dominant firm would have, as users are not able to switch to less intensive, from a data processing perspective, alternatives. The only choice left to users for avoiding this data processing would be to cease using the internet to a large extent or stop using popular services, such as WhatsApp.[190] The BKA does 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, as it is often the case for analysing other exploitative practices, such as excessive pricing.[191] Such economic quantification 'hardly seems possible' in this case. However, this cannot challenge the finding of consumer harm. As the BKA notes, 'it can be assumed that the conduct contested can also lead to potential user harm in economic terms', as '(e)ven the collection of data itself can lead to behavioural changes among users.'[192] Furthermore, the BKA notes that '(u)sers might potentially suffer material (financial) harm if Facebook discloses data to third parties…leading to identity theft, extortion or fraud', but also 'non-material damage' to the extent that the collection of data 'may reveal information that the user considers worthy of protection and which is not provided voluntarily such as income, location, diseases, political views or sezual orientation.'[193]

The potential of harm is even more likely to occur in view of the perverse incentives of the data comptrollers to harvest 'too much data', as they may benefit from the increased monetisation potential of an extensive data collection, while users 'bear the bulk of the potential financial (and intangible) costs incurred.'[194] In any case, the BKA rejected any attempt by a dominant undertaking to justify restrictions of data protection, in particular if these concern the fundamental rights of individuals on the basis of possible positive effects that such violations may bring to its economic performance. According to the BKA, 'the balanced consideration of welfare effects within the framework of the balancing of interests under antitrust law must be countered by the fact that the breach of legal protection provisions which are intended to benefit [195]users cannot be justified.'[196] This indicates that it is not possible for the dominant undertakings to put forward objective justifications to justify the alleged anticompetitive conduct in this case, bringing the approach followed by the BKA close to establishing a per se prohibition, under competition law, for dominant undertakings to violate data protection rules if there is some loose causal link between the infringement of data protection law and the existence of market power.

In the proceedings for interim relief, the OLG Düsseldorf (Higher Regional Court Düsseldorf) however ruled that there were serious doubts as to the legality of the

[189] Ibid., para. 901.
[190] Ibid., para. 903
[191] Ibid., para. 906.
[192] Ibid., para 909. This may hint to the possibility of behavioural harm, explored in Section 8.3.2.2., but the BKA does not provide any further detail as to the way behavioural changes may constitute harm to users.
[193] Ibid., para. 910.
[194] Ibid., para. 911.
[195] See,
[196] Ibid., para. 913.

Bundeskartellamt's orders[197]. The OLG found no exploitative abuse under Section 19(1) GWB. The collection of user and device-related data from the company's other services (Instagram, WhatsApp, Masquerade and Oculus) and Facebook Business Tools, and the aggregation of this data with Facebook data was not held to result in any anti-competitive exploitation of users. The OLG Düsseldorf did not see any indication, that Facebook obtained the users' consent through coercion, pressure, exploitation of a weakness of will or other unfair means, or that the company used the additional data in violation of the agreement beyond the agreed scope. The fact that the use of the Facebook network is linked to the consent to the merging and use of data from other services does not imply any compulsion and does not constitute a predicament for the user. The judgment also focused on the question of whether an abuse of market power by Facebook can be based solely on the assumption of the Bundeskartellamt that the conditions of use at issue violates mandatory provisions of data protection law. The Bundeskartellamt assumed that the infringements of data protection law it had identified was only made possible by Facebook's position of market power. As a result, users would have virtually no option but to agree to the terms of the contract, which constitutes abusive behaviour. The OLG Düsseldorf, however, rejected this assumption on the grounds that an (assumed) violation of data protection law by a dominant company does not necessarily constitute an abuse of market power. The court stated, that the Bundeskartellamt had not sufficiently elaborated why it was Facebook's market power that enabled them to enforce the terms and conditions upon the users. Failing to do so, it is not comprehensible why a contractual partner affected by a data protection law infringement of a dominant company is worthy of protection by competition law while the contractual partner of a non-dominant firm in the same position is not. The court furthermore pointed out that the data provided by the user to Facebook can be endlessly duplicated, which is why the user is not economically weakened by the processing of data. Since the decision of the Düsseldorf Higher Regional Court is based on a request for interim relief, the decision only has a suspensive effect on the orders of the Bundeskartellamt. The order of suspensive effect means that Facebook does not have to implement the Bundeskartellamt's decision for the time being. A final decision by the court is pending, no hearing date has yet been determined. The president of the Bundeskartellamt has announced that the Bundeskartellamt will bring an action before the BGH against the OLG Düsseldorf decision of granting interim relief.

In conclusion, the BKA's Facebook case constitutes one of the first examples of exploitative conduct cases involving UTC and UPC because of its effects on privacy. The authority made efforts to put forward a consistent interpretation of competition law to data protection law and to establish a conceptual framework that would enable the simultaneous application of both areas of law. Concepts of data protection law were repurposed for the occasion so as to match existing concepts and concerns in competition law, taking what has been called by some a strategy of 'cross-institutional isomorphism.'[198]

Of course, the possibility for a specific conduct to fall under another area of law prohibiting abusive contractual or trading terms is always there. And different jurisdictions may arrive to

[197] See, http://www.olg-duesseldorf.nrw.de/behoerde/presse/Presse_aktuell/20190826_PM_Facebook/20190826-Beschluss-VI-Kart-1-19-_V_.pdf .

[198] See, I. Lianos, Polycentric Competition Law, (2018) 71(1) Current Legal Problems 161. 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.'

different choices as to the regulatory strategy to be adopted. For instance, similar types of data harvesting have been sanctioned in Italy on the basis of unfair competition law and consumer protection law.[199]

In the US, additional possibilities are offered through specific tools, such as Section 5 of the FTC Act concerning unfair or deceptive acts 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.[200] In 2011, Facebook settled with the FTC concerning charges that it deceived consumers when it refused to keep privacy promises. In a letter to Facebook on 10 April 2014, the FTC wrote that WhatsApp had notified users about the limited nature of the data it collects and shares with third parties, and highlighted that those promises exceeded the protections that Facebook users enjoy. The FTC wrote to warn Facebook that it must continue to honour WhatsApp's promises to consumers. Any breach could violate Section 5 of the FTC Act[201]. The FTC referred to WhatsApp's privacy policy, dated 7 July 2012, in which WhatsApp indicated the types of data that it 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 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 collects and uses their data. The FTC viewed any failure to keep promises about privacy as a deceptive practice under Sect. 5 of the FTC Act. The FTC further interpreted Sect. 5 as applying when a company uses data in ways that breach promises that had legal effect when it collected the data, unless consumers expressly consent to any changes. WhatsApp's privacy policy stated that it will not utilize customers' information for advertising purposes or sell that information to third parties for commercial or marketing purposes without obtaining users' consent. The FTC recommended that Facebook follow that procedure if WhatsApp begins to collect, use, or share data in a way that is materially inconsistent with the promises in effect when it collected the data. In that situation, consumers should have 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 enjoining Facebook from misrepresenting how it maintains the privacy 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 came also up at 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

[199] See, https://en.agcm.it/en/media/press-releases/2018/12/Facebook-fined-10-million-Euros-by-the-ICA-for-unfair-commercial-practices-for-using-its-subscribers%E2%80%99-data-for-commercial-purposes .
[200] FTC Press Release, *FTC Notifies Facebook, WhatsApp of Privacy Obligations in Light of Proposed Acquisition* (10 Apr. 2014), www.ftc.gov/news-events/press-releases/2014/04/ftc-notifies-facebook-whatsapp-privacy-obligations-light-proposed.
[201] FTC Letter from Jessica L. Rich to Facebook & WhatsApp (10 Apr. 2014), p. 1.

complete the deal.[202] A few years later, the privacy practices of Facebook came again under scrutiny.[203] Users of Facebook reveal intimate information about themselves. A user's 'likes' of public Facebook pages is generally considered as 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. It had emphasized this ability to encourage users to share information. Starting in 2010, each user who installed an app consented, through default settings, to Facebook sharing with the third-party developer that created the app information about both the app user and the app user's Facebook Friends, despite those friends not having installed the app. Affected Friends could opt out of this disclosure only on Facebook's applications page, located on its website. They could not opt out from Facebook's privacy settings page. Third-party app developers provincially used that information to enhance the in-app experience or target advertising to app users and Affected Friends. They could use that information for identity theft, phishing, fraud, and other harmful acts.

In response to a 2012 FTC investigation, Facebook settled claims that sharing Affected Friends data with third-party developers of apps deceived users. The FTC issued an Order that prohibits Facebook from misrepresenting the ability of consumers 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 to its privacy settings page, informing users that concerning the information they share with Facebook Friends, Facebook would make information about both parties available to the app makers. Four months after the FTC finalized the 2012 Order, Facebook removed the disclaimer while continuing to share Affected Friends data with third party developers and while still using the same separate opt-out setting. At a conference in April 2014, Facebook promised that it would cease permitting third party developers to access data about Affected Friends. Facebook informed third party developers that existing apps could continue to collect Affected Friend data for one year, until April 2015. After that date, Facebook arranged with dozens of developers, allowing them to continue to collect 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 data of non-consenting friends with app developers violated the 2012 Order because it replicated the same conduct that the Commission alleged was deceptive in the first count of the original Complaint that prompted the 2012 Order. The 2012 Order mandated that Facebook maintains a reasonable privacy program that safeguarded the privacy, confidentiality, and integrity of user information. This obligation was critical because Facebook was conveying private information from app users and Facebook Friends to millions of third-party app developers. Facebook did not track that data in an organized, systematic

[202] FTC Press Release, *FTC Closes Its Investigation into Facebook's Proposed Acquisition of Instagram Photo Sharing Program* (22 Aug. 2012), https://www.ftc.gov/news-events/press-releases/2012/08/ftc-closes-its-investigation-facebooks-proposed-acquisition.

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

manner. And Facebook did not vet third party developers before bestowing access to consumer data.

The complaint argued that Facebook did not enforce its privacy terms adequately and was rather influenced by the financial benefit that third party app developers provided in return.[204] The severity of any consequences for violating its privacy terms and the speed with which they were administered depended on the financial benefit that Facebook determined that the developer offered to Facebook.[205] The FTC viewed this conduct as unreasonable.

Separate from violating the 2012 Order the complaint argued that Facebook violated Sec. 5(a) of the FTC Act by committing deceptive practices. Facebook had asked users to give personal information to benefit from security measures on the Facebook website or mobile application, including the user's phone number.[206] Facebook used the phone number as part of a two-factor authentication process. It further used the phone number to advertise to users, but never told users about the advertising purpose.[207]

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 utilize the latest facial-recognition technology to identify people in pictures and videos that users uploaded if the user turned the feature on. This suggested that users needed to opt in to use facial recognition. Tens of millions of users who used Facebook with an older version of its facial-recognition technology needed to opt out to disable it. The contrast violated the 2012 Order by misrepresenting how consumers could control the privacy of their information.[208]

Facebook ultimately agreed to pay a $5 billion penalty and incorporate restrictions and a modified corporate structure that the FTC designed to bring more accountability for decisions the company makes about users' privacy. Facebook must create an independent privacy committee situated within Facebook's board of directors. Facebook must certify quarterly that it is complying with the privacy program mandated by the order. And it must review every new or modified product for privacy before implementing it, while documenting its decisions about user privacy.[209]

These issues may also be tackled from a data protection law perspective. These various options should not be considered as substitutes, requiring 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 (e.g. data protection law, unfair commercial practices). Such a toolkit approach may be emulated by other jurisdictions, in particular in the BRICS.

3.2.4. Exploitative requirement contracts

[204] *Id*., paras 88-90.
[205] *Id*., para. 123
[206] *Id*., para. 13
[207] *Id*., paras 142-43.
[208] *Id*., para. 14.
[209] FTC Press Release, *FTC Settlement imposes historic penalty, and significant requirements to boost accountability and transparency* (24 July 2019), https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions.

A possible exploitative theory of harm may result from the analysis of the requirement contracts bundling digital services with personal data provided in 2.1. The standard may be inspired from that employed against exclusionary tying arrangements, although it should cater for the specific theory of harm resulting out of the reduction of privacy standards, manipulation or exploitation of consumers and a reduction of their consumer surplus or well-being. These conditions are the following: (i) the undertaking in question is dominant in the tying market (the market for the 'free product' (e.g. social network, search); (ii) the tying and tied goods are two distinct products (which is of course the case as there is a different market for personal data than that for search or social network services); (iii) the tying practice is likely to have an exploitation effect producing harm to the user – e.g. loss of consumer surplus, wealth transfer, reduction of innovation, reduction of privacy, behavioural manipulation and loss of autonomy; (iv) the tying practice is not justified objectively by efficiencies from which benefit the users (e.g. the data harvested improve the service or product provided to the user, in particular if personalisation has positive welfare effects. As it appears from the above this theory of harm may be standalone or be combined with one of the other theories of harm explored in this Section.

3.2.5. Behavioural manipulation

Although the 'exploitation of attention[210]' and 'attention theft[211]' have been put forward as new forms of exploitative conduct in the digital age, the theoretical contours of these new forms of exploitation have been sketchy, and little has been done as to their operationalisation in the design of competition law standards, in addition to stressing the need for competition law to promote competitive attention markets[212]. This literature lacks for the time being solid foundations on the significant research on manipulation in psychology and raises important questions as to the foundations of human consciousness.

Research in psychology (trait theory) has put forward a Five Factor Model to describe the personality trait structure for all humans and offer some measurement of character[213]. This was first developed by Louis Thurnstone in his 1933 presidential address noting the presence of five independent common factors present in more than 60 trait vocabularies describing personality traits, thus putting forward these five factors as describing the underlying dimensions of personality and temperament: these traits are Extraversion, Neuroticism, Agreeableness, Conscientiousness, and Openness to Experience.[214] The five-factor model assumes that people have transcontextual personality dispositions which are highly stable over time, different situations, and social roles, these traits characterizing 'our very selves.'[215]

[210] T. Wu, *The Attention Merchants* (Atlantic Books, 2016), 23.
[211] T. Wu, The Attention Economy and the Law (March 26, 2017). Antitrust Law Journal, Forthcoming, available at SSRN: https://ssrn.com/abstract=2941094 or http://dx.doi.org/10.2139/ssrn.2941094 .
[212] See, J.M. Newman, Attention and the Law (July 21, 2019), available at SSRN: https://ssrn.com/abstract=3423487 or http://dx.doi.org/10.2139/ssrn.3423487
[213] J.S. Wiggins (ed.), *The five-factor model of personality: Theoretical Perspectives* (Guilford Press, 1996)
[214] L.L. Thurstone, The vectors of mind, (1934) 41 Psychological Review 1.
[215] R.R. McCrae, P.T. Costa Jr, Personality is transcontextual: A reply to Veroff, (1984) 10 Personality and Social Psychology Bulletin 175-17; R.R. McCrae & O.P. John, An introduction to the five-factor model and its

Hence, 'to be true to oneself is to behave in consistent accordance with one's own latent traits.'[216] These five personality trait factors are also universal and transcultural and are linked to the biological unity of humans. Others however 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 result out of 'cohort effects.'[217]

Organismic and existentially informed theories of personality advance a more 'contextual and dynamic view of the person,' 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'[218]. 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.'[219]

Behaviour is therefore function of the personality and the environment (B=f(P, E)[220]. Behaviourists, such as Skinner choose to focus more on the physical environment. Although not rejecting the existence of self (mind), Skinner was more interested in observable behaviour, as opposed to internal events like emotion, arguing that through 'operant conditioning' an individual can make an association between a particular behaviour and a consequence.[221] The concept of reinforcement also emphasises that behaviour which is reinforced tends to be repeated, and thus strengthened, while behaviour which is not reinforced tends to be extinguished (weakened). Behaviour may thus be influenced by reinforcers, as well as by punishers, decreasing the likelihood of the behaviour being repeated. According to behaviourists, through operant conditioning it is possible to modify and shape behaviour, for instance by a system of tokens later exchanged for rewards.

Other approaches focus on internal psychological states, even non-conscious mechanisms. Self Determination Theory (SDT) offers a motivational account of behaviour, which assumes that individuals are active organisms acting on the basis of internal structures and thus making use of both their internal and external environments. Motivation relates to

---

applications, (1992) 60 Journal of Personality 175; R.R. McCrae & P.T. Costa Jr, The stability of personality: Observations and evaluations, (1994) 3 Current Directions in Psychological Science 173.

[216] K. M. Sheldon, R. M. Ryan, L. J. Rawsthorne, & B. Ilard, Trait Self and True Self: Cross-Role Variation in the Big-Five Personality Traits and Its Relations With Psychological Authenticity and Subjective Well-Being, (1997) 73(6) Journal of Personality and Social Psychology 1380.

[217] R.B. Cattell, The description of personality. 1. Foundations of trait measurement, (1943) 50 Psychological Review 559; R.B. Cattell, The description of personality: Basic traits resolved into clusters, (1943) 38 Journal of Abnormal and Social Psychology 476.

[218] K. M. Sheldon, R. M. Ryan, L. J. Rawsthorne, & B. Ilard, Trait Self and True Self: Cross-Role Variation in the Big-Five Personality Traits and Its Relations With Psychological Authenticity and Subjective Well-Being, (1997) 73(6) Journal of Personality and Social Psychology 1380, 1380.

[219] Ibid. citing A.S. Waterman, Personal expressiveness: Philosophical and psychological foundations, (1990) 11 *Journal of Mind and Behavior* 47; R.M. Ryan, Agency and organization: Intrinsic motivation, autonomy and the self in psychological development, in J. Jacobs (ed.), *Nebraska Symposium on Motivation: Developmental perspectives on motivation* (Vol. 40, University of Nebraska Press, 1993) 1; E.L. Deci & R.M. Ryan, *Intrinsic motivation and self-determination in human behaviour* (Plenum Press, 1985).

[220] K. Lewin, Behavior and development as a function of the total situation, in L. Carmichael (ed.), Manual of child psychology (Wiley, 1946), 791.

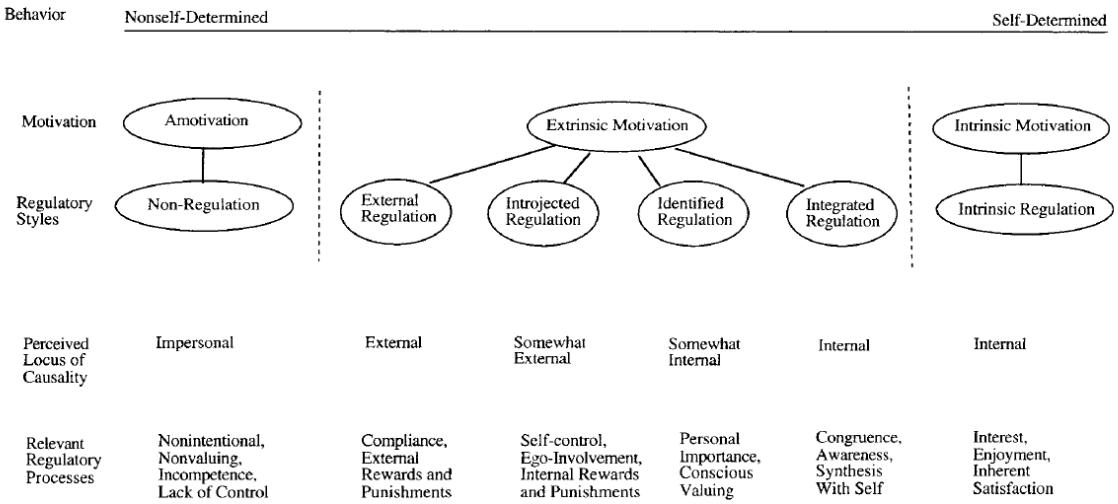
[221] See, B.F. Skinner, *The Behavior of organisms: An experimental analysis* (Appleton-Century, 1938); B.F. Skinner, *Science and human behaviour* (Simon and Schuster 1953).

'energy, direction, persistence and equifinality; characterizing activation and intention.[222] Hence, human motivation may be intrinsic, human beings when performing an activity making use of internal structures which form part of their perception of the phenomenal core of the *self*, as well as extrinsic, to the extent that human behaviour occurs for reasons other than the activity itself. SDT theory makes a distinction between 'autonomous motivation', which comprises both intrinsic motivation and the types of extrinsic motivation in which people have identified with an activity's value and ideally will have integrated it into their sense of self', thus experiencing a 'self-endorsement of their actions', and 'controlled motivation' which, in contrast, '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 internalized and is energized by factors such as an approval motive, avoidance of shame, contingent self-esteem, and ego-involvements.'[223] Behaviour is energized and directed by both autonomous and controlled motivation, the lack of motivation and intention marking the other pole (amotivation). Psychologists distinguish six categories of regulation of an activity in the self-determination continuum, in view of the respective role of intrinsic and extrinsic motivation (external regulation) (see Figure 11.1.):

- *Amotivation*: there is no intention to act;
- *External Regulation*: which denotes extrinsically motivated behaviour which is performed to satisfy an 'external demand or reward contingency', individuals typically experiencing such behaviour feeling controlled or alienated, their actions being perceived by them as having an external locus of causality
- *Introjected Regulation*: involves taking in external regulation but 'not fully accepting it as one's own', the behaviour being performed 'to avoid guilt or anxiety or to attain ego enhancements such as pride';
- *Identified Regulation*: involves 'a conscious valuing; of a behavioural goal or regulation and represents a 'more autonomous, or self-determined, form of extrinsic motivation';
- *Integrated Regulation*: when regulation is 'brought into congruence with one's other values and needs, and thus fully assimilated to the self.
- *Intrinsic Regulation*: is marked by fully intrinsic motivations, the subject doing an activity for its 'inherent satisfactions'[224]

Figure 1.: The Self Determination Continuum

[222] R.M. Ryan & E.L. Deci, Self-Determination Theory and the Facilitation of Intrinsic Motivation, Social Development and Well Being, (2000) 55(1) American Psychologist 68, 69.
[223] E.L. Deci & R.M. Ryan, Self-Determination Theory: A Macrotheory of Human Motivation, Development, and Health, (2008) 49(3) Canadian Psychology 182, 182.
[224] R.M. Ryan & E.L. Deci, Intrinsic and extrinsic motivations: Classic definitions and new directions, (2000) 25 Contemporary Educational Psychology 54.



Source: R.M. Ryan & E.L. Deci, Self-Determination Theory and the Facilitation of Intrinsic Motivation, Social Development and Well Being, (2000) 55(1) American Psychologist 68, 72

An 'enormous amount' of research, including empirical, shows that autonomous motivation, which we can locate as including the categories of intrinsic motivation, integrated regulation and identified regulation, 'tends to yield greater psychological health and more effective performance on heuristic types of activities.'[225] Research shows that 'there is a set of universal psychological needs that must be satisfied for effective functioning and psychological health', in particular the needs for competence, autonomy and relatedness, which 'predict psychological well-being in all cultures', with no difference for cultures valuing individualism and those valuing collectivism.[226] There is also evidence that a controlled regulation environment depletes energy and may affect vitality, and thus performance. Hence, options should be offered to users in a non-controlling way, if we are to preserve rather than undermine autonomy. Even if law and policy may only impact on one only dimension of the broader environment affecting an individual's autonomy, research in psychology may provide a lot of wisdom for the definition of possible theories of user/consumer harm in competition law, thus providing some relief from corporate conduct that reduces autonomy.

Self-determination and autonomy may be reduced by active manipulation by corporations of consumers' biases.[227] Manipulation may take a more industrial scale in digital markets. This has led to an emerging body of scholarship attempting to define manipulation in

[225] E.L. Deci & R.M. Ryan, Self-Determination Theory: A Macrotheory of Human Motivation, Development, and Health, (2008) 49(3) Canadian Psychology 182, 183. See also G.A. Nix, R.M. Ryan, J. B. Manly, E.L. Deci, Revitalization through Self-Regulation: The Effects of Autonomous and Controlled Motivation on Happiness and Vitality, (1999) 35(3) Journal of Experimental Social Psychology 266; V. I. Chirkov, R. Ryan, K. M. Sheldon, *Human Autonomy in Cross-Cultural Context: Perspectives on the Psychology of Agency, Freedom and Well-Being* (Springer, 2011).

[226] E.L. Deci & R.M. Ryan, Self-Determination Theory: A Macrotheory of Human Motivation, Development, and Health, (2008) 49(3) Canadian Psychology 182, 183.

[227] J D. Hanson & D A. Kysar, Taking Behavioralism Seriously: The Problem of Market Manipulation, (1999) 74 New York University Law Review 630.

both offline and online contexts,[228] but also some concerns expressed by regulators[229]. Calo expressed the problem of self-determination and autonomy of digital consumers as linked to the mediating role of technology, which enables some business actors 'to design every aspect of the interaction with the consumer.'[230] One may certainly envision manipulation as involving an intervention that changes the way someone behaves. Hence, but-for this intervention the person would have behaved differently. Susser et al note that intervention may, in abstract, take the following two forms: (i) change the 'decision space' of an individual, for instance by changing the options available to them, and (ii) change 'their internal decision-making process', in order words, 'the way they understand their options.'[231]

The difficulty consists in determining what distinguishes manipulation from other forms of intervention, such as simple influence or persuasion. The latter does not raise concerns with regard to self-determination and autonomy as it makes an appeal to the person's decision-making power. Spencer defines manipulation as 'an intentional attempt to influence a subject's behaviour by exploiting a bias or vulnerability.'[232] The manipulator targets the individual's capacity for self-government 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.'[233] The intent of the alleged manipulator is a factor emphasised by the literature.[234] Similarly, the hidden nature of the manipulative influence ensures that the manipulated person is unaware of this external regulation, thus excluding situations of introjected regulation from being considered as manipulation. Susser et al argue 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 in order to steer his or her decision-making process towards the manipulator's ends.'[235] These may be cognitive biases, or emotions and desires.

These authors also consider that deception does not constitute a necessary condition for manipulation, as there might be manipulation without deception. Similarly, nudging can be

---

[228] See, in general, R. Calo, Digital Market Manipulation, (2014) 82 George Washington Law Review 995; E.A. Posner, The Law, Economics, and Psychology of Manipulation (June 11, 2015). University of Chicago Coase-Sandor Institute for Law & Economics Research Paper No. 726, available at SSRN: https://ssrn.com/abstract=2617481; F.Z. Borgesius, *Improving Privacy Protection in the Area of Behavioural Targeting* (Kluwer Law International, 2015); T.Z. Zarsky, Privacy and Manipulation in the Digital Age, (2019) 20 Theoretical Inquiries in Law 157; S.B. Spencer, The Problem of Online Manipulation (March 12, 2019), available at SSRN: https://ssrn.com/abstract=3341653 ; D. Susser, B. Roessler, H.F. Nissenbaum, Online Manipulation: Hidden Influences in a Digital World (December 23, 2018), available at https://ssrn.com/abstract=3306006 .

[229] European Data Protection Supervisor, Opinion 3/2018, EDPS Opinion on online manipulation and personal data (March 19th, 2018), available at https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf .

[230] R. Calo, Digital Market Manipulation, (2014) 82 George Washington Law Review 995, 1003-1004.

[231] D. Susser, B. Roessler, H.F. Nissenbaum, Online Manipulation: Hidden Influences in a Digital World (December 23, 2018), available at https://ssrn.com/abstract=3306006 , 11

[232] S.B. Spencer, The Problem of Online Manipulation (March 12, 2019), available at SSRN: https://ssrn.com/abstract=3341653 , 4.

[233] D. Susser, B. Roessler, H.F. Nissenbaum, Online Manipulation: Hidden Influences in a Digital World (December 23, 2018), available at https://ssrn.com/abstract=3306006 , 15.

[234]

[235] D. Susser, B. Roessler, H.F. Nissenbaum, Online Manipulation: Hidden Influences in a Digital World (December 23, 2018), available at https://ssrn.com/abstract=3306006 , 2. For a different position, see C. Sunstein, The Ethics of Influence: Government in the Age of Behavioral Science (Cambridge Univ. Press, 2016), 102-105.

manipulative, but not all nudges are manipulative. Susser et al. Finally, coercion restricts acceptable options from which another person may choose, and constitutes a more direct intervention of external regulation of behaviour than manipulation. The same authors argue that the digital economy facilitates manipulation as it enables digital platforms to harvest and analyse personal data enabling them to identify more easily consumers' weaknesses and vulnerabilities: they can reach over various dimensions of human experience, and they are 'dynamic, interactive, intrusive' and set forth 'incisively personalizable choice architectures' that may steer consumer choice.[236] The subversion of the decision-making power of individuals through manipulation challenges their autonomy and self-determination, with harmful effects on their development and productivity. It also raises broader concerns if manipulation in consumer markets may be easily converted to power in the political sphere. Psychographic profiling identifying with increasing levels of accuracy personality traits becomes the new normal in the data economy, driving business practices and enabling targeted forms of advertising at the individual consumer level without any comparison, in terms of effectiveness, with regard to the tools of traditional advertising.

Prior to accepting the claims for manipulation lays a more fundamental debate, that of the nature of human consciousness. Phenomenology and Cartesian thinking insists on the distinction between the brain and the mind, carefully distinguishing an 'internal' from an 'external' world, dividing our phenom in three parts: '(i) 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'; (ii) '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'; and (iii) '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'[237]. This approach distinguishes between the brain where various of these stimuli are processed, and the 'self', the 'centre of narrative gravity', the latter being forming the 'core' of a person and the foundation of its autonomy. However, others have put forward a 'Multiple Drafts' model, where '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', 'information entering the nervous system' being 'under continuous "editorial revision"'[238]. These authors emphasise the development of streams of content that are subject to 'continual editing by many processes distributed around in the brain, and continuing indefinitely into the future', without there being a 'single narrative' (a 'final' or 'published' draft)[239], as understanding is a property that 'emerges from lots of distributed quasi-understanding in a large system'[240]. 'Probing this stream at various intervals produces different effects, precipitating different narrative-and these

[236] D. Susser, B. Roessler, H.F. Nissenbaum, Online Manipulation: Hidden Influences in a Digital World (December 23, 2018), available at https://ssrn.com/abstract=3306006 , 2.
[237] D.C. Dennett, *Consciousness Explained* (Back Bay Books, 1991), 45.
[238] Ibid., 111.
[239] Ibid., 113.
[240] Ibid., 439.

are narratives'[241]. 'Any narrative… that does get precipitated provides a "time line", a subjective sequence of events from the point of view of an observer'[242]. This theory may raise interesting questions as to the definition of what 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. The approach and its empirical foundations have been subject to criticism and the conclusions reached may not hold[243], hence the need for more research and debate.

Defining the various parameters of the concept of manipulation affecting human consciousness is not the only challenge; it is also important to determine what would be the acceptable sources of evidence for manipulation and to design an appropriate test drawing not only on economics and behavioural economics but also psychology. This should be an important task for the future for competition authorities and academia.

3.3. Remedies

We are in favour of collective action to restore the conditions of a well-functioning data market. In the model we presented, in regime 2, we assumed that in the opt-out world there was significant competition so that the purchaser of personal information is forced by competition to offer $y, the full value of the personal information to the company. If such competition among purchasers of personal information were not present, and, for example, Google remained a monopsonist as in regime 3, the user would not be appreciably better off in the opt-out world rather than the opt-in world. So, a remedy cannot be just the change from opt-in to opt-out, but has to accomplish or at least imitate competition in the market for personal data sale.

A possible solution dealing with the risk that users are imposed conditions to which they did not provide they voluntary consent is that the 'default' regime be changed from 'opt-in' to 'opt-out.' Applying these principles to the case of social networks, one may argue that Facebook has no incentive to make this change on its own, and therefore this has to be achieved by regulation. This is certainly the choice made by the EU when adopting the GDPR, which put in place an 'opt out' regime. However, even if one changed to 'default opt-out', this will not have provided an adequate response, as the dominant social network may impose, because of its market dominance, the conditional use of the website to the 'consent' provided by the users of their data being harvested. Hence, an 'opt-out regime' will not be enough because of the asymmetrical bargaining power between the digital platforms enjoying a dominant position and the users.

One option may be to mandate that the digital platform offer the same product by asking for a fee, if data is not to be harvested and the users not being subject to targeted advertising. In cases in which the data of the specific user is quite valuable, it would be possible to require

[241] Ibid., 135.
[242] Ibid., 136.
[243] See, for instance, K. Akins, Lost the Plot? Reconstructing Dennett's Multiple Drafts Theory of Consciousness, (1996) 11(1) Mind and Language 1.

the digital platform to provide a positive payment to these users so that they can join the social network. Again this will raise several issues.

First, because of its dominant position Facebook may deny users 'free' access to its services if they opt to exercise their privacy rights, it may overcharge users or not pay them the competitive price to join the social network or to 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, much higher profitability for large size network, barriers to entry for new networks, as well as providing the ability of a larger network to subsidize some 'influential' users to subscribe.

Second, another issue is, as mentioned in Section 2.5.. the missing market that would enable users to evaluate the full cost and benefit of their transaction with Facebook. Once we understand the interaction between user and Facebook/Google as a *market* interaction we may fully grasp the possibility that the dominant position of the buyer of data (monopsony) may lead to inefficient exchanges, or that the monopsony buyer may have a lot of user-specific information and can implement sophisticated price discrimination strategies.

This calls for antitrust enforcement, in particular conduct as well as structural remedies, privacy regulation, but also other regulatory tools that would aim to set up a market between users and the network, ensure the transparency in the collection of data (so that users know what is collected), ensure ttransparency in the use of data (so that users know how their data is used), and ensure user's consent in data collection and specific use eventually with a possible compensation to the user for 'selling' his data to a company like Google or Facebook.

Such regulation should also make 'opt-out' the default. If a user opts-out, Facebook or Google should not be able to use or sell the data the user discloses to Facebook/Google. Users may be compensated for opting-in, thus allowing Facebook/Google to harvest the user's raw data as well as his 'activities' and 'connections.' This default opt-out will create a *market* between the user and Facebook or Google, where the user sells his data to the digital platform. More concretely, with regard to Google, opt-out should be the default for browsers Android, and Google search. Users should have opt-out choice for other personal data, such as health data, even if this data was not acquired from the users. Users may also be able to easily set their browser to delete cookies and trackers at end of use/session and users should be able to avoid Chrome.

This opens the possibility for a possible compensation to the user for 'opting-in' that is, for 'selling' his data to a company like Google or Facebook. Depending on the extent that a user opts-in, he may be compensated in different amounts for allowing

- collection ("opt-in") of his personal data directly from the company he interacts with (say Google);
- use of his data for a specific purpose by Google (say for marketing vs political campaigns);
- sale of data to third parties by Google.

The EU takes a different perspective as pricing remains unaffected by the opt-in/opt-out decision.

Pricing the data should nevertheless avoid the pitfall of letting the monopolist/dominant digital platform use its superior bargaining power vis-à-vis individual users to ask for the

monopsony price (in terms of data harvesting). This raises the question of identifying the but-for the infringement world, in order to determine the competitive monetary value of the data and thus ensure the proper payment of the users (if positive prices are charged), or the amount the users should be asked to pay (in data value or monetary prices) in order to have access to 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 at a comparable, in terms of relevant characteristics, geographic market which is nevertheless significantly more competitive than the market under examination.

Several other remedial options exist in order to restrict the privacy-harming potential of digital platforms with market power. It might be possible to break up the platforms horizontally by introducing in the market several horizontal competitors. However, one may observe the relatively low effectiveness of this remedy in view of the 'winner takes most competition' effect in markets with intensive network effects. Even if there are new entrants in this market, the resulting market structure may not be significantly different and competition will be 'for the market' rather than intensifying 'competition in the market', at least in the medium to long term. A vertical separation of the platform from the merchants, by prohibiting them to expand in vertically related markets may also provide some temporary relief, but may also slip to some form of detailed regulation, a hybrid between utilities' regulation and data protection/privacy regulation. Of course, this may become an acceptable option in some circumstances.

Platforms may opt to pay for the users' data thus leading to the emergence of a licensing market for user data for users opting-in to share their data with the platforms. At the same time this enables the users to port this data to platforms offering them a higher return and better conditions in terms of higher value for their privacy (e.g. lower data input for equivalent, in terms of quality, search output).

Exclusive licencing of personal data to a company will imply a monopsony and will not solve the problem of competition in the personal data market. We could institute non-exclusive licensing through a licensing agency that would collect the data from each user and distribute it to platforms. The user would be paid the sum of the willingnesses to pay of all the company bidders. However, what determines how much a user gets paid or pays? Assuming similar competing networks, a user would like a larger network because there are more possibilities of interaction, and therefore his willingness to pay $x increases in the size of the network. If we assume that the influence of a user is on a finite number of friends, a smaller network would be willing to pay more to add him, so $y does not increase with network size, for networks above a moderate size. Additionally, a dominant network will be able, in general, to pay users less and/or demand higher payments from users, because of the use of its market power, and of the information about the features of the users. So, we expect that most users will pay more to subscribe in a large and dominant network and be paid less by it. In order to determine what will constitute a 'fair' value one will need to refer to the value in a competitive market. However, this is not possible in the specific case as there is no perfectly competitive market and there cannot be one because of network effects. Digital platforms may exercise their buying power leading to a downward pricing pressure in the market for personal data for input suppliers (the users) and therefore deprive them from a portion of their revenues. Because of the buying power of digital platforms (or the monopsony they may benefit from) and the fact

that this sorry situation results from the initial requirement contracts bundling digital services with personal data competition law should grant to the users a legitimate interest in prices which shall not be 'artificially' low. In some jurisdictions, low pricing may be found to be unfair pricing and therefore infringe the abuse of dominance provisions[244].

A possible solution to this problem is for NCAs to facilitate the users to collectively bargain with the platforms rates for the payment they will receive for the data harvested in order to protect their personal data.[245] The value of personal data and therefore the price to which these may be sold to digital platforms may also increase by some input limitations by a digital and/or data protection regulator as to the amount of data to be harvested. It could also be limited by collective bargaining between privacy-prone users (if the number of users with strong preferences for privacy is significant) and the digital platforms, eventually through the constitution of collecting societies by the various groups of users that would also bargain with the digital platforms. One may consider the existence of one collecting society or several representing different preferences for privacy protection, assuming consumer preferences about privacy are heterogeneous.

Additional remedies that may address the problem of the lack of a market for personal data is data portability providing users the ability to export their social graph or their search history.

Interoperability remedies may also intensify inter-platform competition. For instance, Facebook should change from a closed to an open communication network enabling its users to also send messages to users of other social networks. This would require the adoption of an open API for user messages, chats, posts, and other communications.

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 aims of the adds-based business model, such as adding Adblocks[246] and the development of tracking protection technologies[247]. For instance, NCAs may mandate the development of a unique 'Do not track' switch that may apply for all networks and prohibit or even bring abuse of dominance cases for exploitation

---

[244] Unfairly low prices may also be a concern for the application of Article 102(a) TFEU. This does not concern predatory prices, but situations in which a dominant buyer purchases inputs at unfairly low prices. These are determined according to a comparison between the price paid and the economic value of the service provided. In *CICCE*, the CJEU examined an action for annulment against a decision of the Commission relating to conduct by some French television stations holding exclusive broadcasting rights to pay low license fees for the rights of films and accepted that article 102(a) 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 yardstick valid for all firms, since each film is different: Case C-298/83 *Comité des industries cinématographiques des Communautés européennes v Commission* [1985] ECR 1105. This type of theory of harm is more difficult to implement in the US, where since the Weyerhaeuser case of the Supreme Court in view of the high standards required for a successful claim of predatory bidding (the SCOTUS stipulating that the *Brooke Group* predatory pricing analysis applies equally to the predatory pricing of outputs and predatory bidding for inputs). Since this case, however, the US antitrust authorities, and more generally the US antitrust community, have shown more openess of mind for such claims and in particular shown concern for monopsony power in antitrust and merger control (in specific sectors, such as agriculture, but also beyond). See, J. Shively, When Does Buyer Power Become Monopsony Pricing?, (2012) 27(1) Antitrust 87; C.S. Hemphil & N.L. Rose, Mergers that Harm Sellers, (2018) 127 The Yale Law Journal 2078.

[245] See, https://www.economist.com/the-world-if/2018/07/07/data-workers-of-the-world-unite .

[246] See, https://iapp.org/news/a/the-privacy-consequences-in-the-rise-of-ad-blockers/

[247] See, https://blog.mozilla.org/blog/2019/06/04/firefox-now-available-with-enhanced-tracking-protection-by-default/ and https://www.wired.com/story/privacy-browsers-duckduckgo-ghostery-brave/ .

against Facebook or Google if they try to bypass these technologies or forbid their use in their platforms[248].

4. Conclusion

The paper explores a market failure approach in thinking about restrictions to competition by digital platforms affecting privacy, and the possibilities of enforcing competition law against these type of restrictions. We analyse the various ways of action and argue for the development of new categories of exploitative practices, both in *ex ante* and *ex post* enforcement. We are in favour of collective action, through competition law enforcement, to restore the conditions of a well-functioning data market and the paper makes the following policy recommendations:

- Reflect on broader guiding principles on privacy-related competition law theories of harm (from a market failure perspective).
- Establish new theories of exploitation in the context of abuse of dominance law
- Explore legislative intervention changing the 'default' regime for data harvesting from 'opt-in' to 'opt-out' if the specific jurisdiction disposes of a data protection regime. This opens the possibility for a possible compensation to the user for 'opting-in' that is, for 'selling' his data. This may facilitate the emergence of a licensing market for user data for users opting-in to share their data with the platforms, thus dealing with the 'missing markets' problem and its associated effects.
- Facilitate the users to collectively bargain with the platforms rates for the payment they will receive for the data harvested in order to protect their personal data, thus neutralising the asymmetrical bargaining power of large digital platforms and digital giants.
- Promote 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 aims of the adds-based business models.

[248] 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 https://www.inc.com/jason-aten/google-is-putting-an-end-to-ad-blocking-in-chrome-here-are-5-best-browser-alternatives.html .