The intersection between Antitrust and Data Protection

Lessons from the Facebook/Whatsapp merger and the Bundeskartellamt's decision on Facebook's terms and conditions

Author : Rancati Luca

Thesis Director : Elisabeth de Ghellinck

Thesis Reader : Alexandre de Streel

Academic Year 2018-2019

In order to obtain the joint degree:

Master 120 en Sciences économiques, Orientation générale, Finalité spécialisée (UCL/UNamur)

and

Dottore magistrale in Economics and Political Science (UNIMI)

Université catholique de Louvain - Economics School of Louvain - Place Montesquieu 3, 1348 Louvain-La-Neuve
Université de Namur – Economics School of Namur – Rempart de la Vierge 8, 5000 Namur
Università degli Studi di Milano • Via Festa del perdono 7 • 20122 Milano / Italy

Abstract

Most of the digital products are paid by users and consumers online with the provision of their personal data, so a complex parameter of competition is getting more and more attention in the assessment of online platforms antitrust cases: privacy. This transaction has always been considered principally under data protection authorities' jurisdiction but has slowly become crucial in many antitrust cases on both sides of the Atlantic Ocean. In this work we investigate this intersection between competition law and privacy law. We try, on one side, to identify some tools potentially available to implement privacy concerns in antitrust, and on the other side to highlight which are the consequences on the two agencies enforcement.

In Section I, the technological and juridical nature of personal data is presented. We then explain the factors and market dynamics which make them a relevant competitive and strategic asset. In section II, we analyse the concepts of "Privacy Paradox" and "Privacy Calculus" which together justify the common view on online consumers' behaviour: if the market is not promoting online privacy-enhancing technologies, it is because consumers don't really signal this need with consistent preferences. Finally, in Section III, we will analyse two cases: the Facebook/WhatsApp merger cleared by the European Commission in 2014 and the Bundeskartellamt's decision on Facebook abusive terms and conditions, published on the 11th July 2019. In both cases privacy is a crucial parameter of competition. In the first case, we will see how the Facebook/WhatsApp investigation could have been enhanced by a conception of privacy as "non-monetary price" and a coherent privacy-related theory of harm. The latter case, is instead interesting for the unprecedent approach adopted by the German Authority, paving the way for a new consideration of privacy and personal data. The case is hotly debated and may start a closer and innovative collaboration between competition agencies and data protection ones.

Acknowledgments

I want to express my sincere thanks to my Supervisor Professor Elisabeth De Ghellinck for the precision and patience showed to me through all the writing of this memoire, to my Reader Professor Alexandre de Streel, and to my co-Reader from the University of Milan Professor Massimiliano Bratti.

I would like to thank my friends: Alessandro who shared with me the joys and struggles of this common path, from Milan to Louvain-La-Neuve. I owe him a lot; Lorenzo for his contagious positivity and brightness.

Special thanks to Monique for all the support and for all the things she has done for me. Time goes faster when I am with you.

Finally, my deep gratitude goes to my family, for the unconditional love and hep they always given to me in countless ways. Thank you.

Index

I- The Interplay between competition and privacy

1. Introduction

In 2019, the world of antitrust and data protection authorities has been characterised by some unprecedent events which are paving the way for a discussion (and maybe an overcome?) of certain consolidated practices whose effectivity is now starting to get doubted. The two occurrences we are talking about are the recent fine imposed by the FTC to Facebook for the Cambridge Analytica case[1], which is the highest one ever in the history of the American authority (five billion USD), and the Bundeskartellamt investigation ended in February, which found Facebook's services terms and conditions of use abusive. The two decisions refer to different types of infringements: in the Cambridge Analytica scandal, it is a pure data protection violation. The case had a huge resonance worldwide and put Facebook under the spotlight of public opinion and politicians for months during last year. Being linked to Donald Trump campaign in the US elections, the scandal became the most evident exemplification of the incredible level of power and influence reached by digital platforms (in particular those tech giants commonly known as GAFAM[2]) in our society. The Facebook's conduct was so bold and contemptuous of internet users' rights that it is now irresponsible for authorities to overlook the situation and not to take some decisive resolutions.

On the other side of the Atlantic, the German competition authority, the Bundeskartellamt, raised a new debate after the publication of its investigations results in February[3]. Here, the attention received doesn't depend on the requirements imposed to the company, but rather on the methodology and on the theoretical ground adopted by the authority. It is the first time that an abuse of dominance is grounded on the violation of data protection rules. This case, which constitutes an absolute novelty, is discussed in details in the third section of our work.

What is the link between these two events, apart from their temporal closeness and their mediatic relevance? They are both strongly pivoted on privacy law and data protection rules. However, despite this evident common feature, the Bundeskartellamt's resolution constitutes a "vanguard", and that's the reason why it is the only one we will treat. The investigation addresses (not without some complexities and flaws) what appears more and more to be an unavoidable issue: the intersection between privacy and market power in the online digital market. Competition law and privacy law are entangled by the business structure underlying most of the data-driven multi-sided services currently on the digital market. Users on the free side of the platform pay products and services by exchanging personal information and data. Name, age, email address, gender, political opinions, geo-localization, friends network, activity records and ratings are the currency each of us is using to pay while using an

[1] Cecilia Kang, *F.T.C. Approves Facebook Fine of About $5 Billion,* The New York Times, 12 July 2019. https://www.nytimes.com/2019/07/12/technology/facebook-ftc-fine.html

[2] Google, Amazon, Facebook, Apple and Microsoft. Nowadays, another acronym is spreading, referring to the Chinese giants "BATX": Baidu, AliBaba, Tencent and Xiaomi.

[3] A case summary and a FAQs press release were initially published on the 6th of February. The full-length decision has been recently released too. Accessible at: https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/AktuelleMeldungen/2019/11_07_2019_decisionFacebook.html

app, a social network, a search engine and many others services. It is an actual form of payments, a transaction, and users are still not completely aware of the real value of their personal data.

The purpose of this work is to investigate this transaction and to understand which are the implications in terms of competition law and antitrust authorities' practices. We will follow the red line drawn by the Bundeskartellamt's decision and show how the competitive dimension of privacy protections could have been noteworthy in another important case related to Facebook: the merger with WhatsApp cleared in 2014 both by EU[4] and US agencies.

Far from having the presumption to propose a solution, we will explore and deepen the possibilities and tools available to enforcers once this intersection between antitrust priorities and privacy rules is embraced. In the first section, we analyse the nature of personal data, as they are defined by European GDPR, and we will develop all the features which give them a competitive relevance in chapter 3, 4 and 5. The second section takes a step into the field of Economics of Privacy. It focuses, in particular, on the so-called Privacy Paradox, which is a central theoretical issue concerning online and offline agents' behaviour. The subjective, multi-dimensional and intangible nature of privacy preferences is what makes difficult the assessment of consumer welfare in many antitrust cases. Privacy is a non-monetary parameter of competition and suffers many of the intrinsic operative complexities common to that category. A brief overview of the economic literature on disclosure/protection of personal information will help us to grasp the essential theoretical background informing all the discussion. We will see that, until now, there is no clear and common evidence on efficient equilibria benefitting both data subjects and data holders. The outcomes are highly context-dependent and biased by many existing information asymmetries, behavioural factors and deceptive artificial designs. Finally, in the third section, the elements presented previously will get altogether and will be the basement to build the analysis of two antitrust cases deeply related to privacy issues: the Facebook/WhatsApp merger in chapter 11, and the Bundeskartellamt's investigation on Facebook in chapter 12. The former case study is an opportunity to check the possible operative contribution to antitrust analysis deriving from a stronger attention to privacy issues. We will try to discuss some tools and techniques able to give a new perspective on the case, and to understand which parts of the European Commission resolution might have been changed by a more competition-oriented view of data protection matters.

The latter more recent case is generating a huge debate. We will analyse the methodology and the economic analysis developed by the Bundeskartellamt, trying to evidence strong and weak points of the decision. Is the resolution taken by the German authority applicable outside German borders? Will it remain unique or does it have external validity? Is it possible to justify it under art.102 of TFEU and not only under German law? Even here, it is not possible to give definitive answers. The decision has been appealed by Facebook and it is still too early to clearly evaluate the consequences. Nonetheless, the potential effects of this vanguard decision on the relationship between data protection agencies and competition agencies will be part of our discussion. The incumbent European Data Protection Supervisor, Giovanni Buttarelli, has welcomed enthusiastically the results of the investigation and has expressed his satisfaction about seeing data protection rules becoming a benchmark for competition law enforcers[5]. However, it is evident (for Mr. Buttarelli too) that this new implied "partnership"

[4] The full text of the European Commission is available at: http://ec.europa.eu/competition/elojade/isef/index.cfm?fuseaction=dsp_result&case_title=FACEBOOK. The FTC didn't release any document to explain the clearing of the case.

[5] G. Buttarelli, *This is not an article on data protection and competition law*, CPI Antitrust Chronicle, 2019

between the agencies can be problematic both from a pure operative and jurisdictional point of view and from a more specific theoretical and legal perspective.

2. Personal data

Personal data are a unique category of Big Data, they have specific features and they are accurately defined by complex legal frameworks, as the General Data Protection Regulation. In this chapter we will present them in all their main characteristics, we will differentiate them from non-personal data and subdivide them in different sub-categories. All these distinctions are legally important and allow us to have a complete and detailed understanding of what is the "main protagonist" of this work. The presentation of the specific typologies of data, and the different kind of technological procedures they are subject to, will allow us to better understand the privacy risks related to the collection, storage, transmission and usage of these data. Nonetheless, in this first chapter, it will be already possible to grasp why, given their incredible level of precision and accuracy, these data are so valuable and precious for online services and firms.

2.1 What are personal data?

The General Data Protection Regulation (GDPR)[6] defines personal data as follows: "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person"[7]. Some examples of different types of personal data[8]:

- User generated content, including blogs and commentary, photos and videos, etc.
- Activity or behavioural data, including what people search for and look at on the Internet, what people buy online, how much and how they pay, etc.
- Social data, including contacts and friends on social networking sites;
- Locational data, including residential addresses, GPS and geo-location (e.g. from cellular mobile phones), IP address, etc.
- Demographic data, including age, gender, race, income, sexual preferences, political affiliation, etc.
- Identifying data of an official nature, including name, financial information and account numbers, health information, national health or social security numbers, police records, etc.

[6] GDPR entered in application in May 2018 https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en

[7] 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. Available at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

[8] OECD (2013), Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value, OECD Digital Economy Papers, No. 220, OECD Publishing, p.8

Personal data have been categorised in different ways by research literature. For example, Schneier[9] in a 2010 OECD workshop differentiated six types of personal data: service data, needed to open an account (i.e., name, address, credit card information, etc.); disclosed data, entered voluntarily by the user; entrusted data, like the comments made on other people's entries; incidental data, which is about a specific user, but uploaded by someone else; behavioural data, deriving from users navigation of a website and used for targeted advertising; and inferred data, which is deduced from users' disclosed data, profile and activities[10].

Personal data can be also categorised according to its use. It is common to distinguish between data collected by a particular entity for use during the current Internet session (referred to first-party use) and that which is stored for use and analysis over time and/or sold on to third parties (third-party use)[11]. The table below illustrates the impressive amount of data types collected on consumers, based on the combined findings from the UK Competition and Markets Authority (2015)[12] and Rao et al.[13].

Figure 1: Data collected by firms for commercial purposes[14]:

Data category	Examples of type of data collected per category*
Data related to social relationships	▪ Links between family members and friends
Open data and public records	▪ Birth and death records ▪ Marriages ▪ Electoral registers ▪ Court and insolvency records ▪ Land registry records
Data transmitted online /stored by users on devices or the "cloud"	▪ Audio-visual media (e.g. photos, videos etc.)

[9] OECD (2010), *The role of Internet Intermediaries in Advancing Public Policy Objectives*, Workshop, Paris June 2010, OECD DSTI/ICCP(2010)13, p.14

[10] OECD (2013), *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD Digital Economy Papers, No. 220, OECD Publishing, p.8

[11] (FTC, 2009)

[12] Competition & Markets Authority (2015), "*The commercial use of consumer data*", Report on the CMA's call for information. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/435817/The_commercial_use_of_consumer_data.pdf

[13] Rao A., Schaub F. and Sadeh N., (2014), Carnegie Mellon University: "What do they know about me? Contents and concerns of Online Behavioural Profiles". Available at: https://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab14011.pdf

[14] European Commission Report, *Consumer market study on online market segmentation through personalised pricing/offers in the European Union final report*, 2018. The list does not have the presumption to be exhaustive

Data category	Examples of type of data collected per category*
Financial and transactional data	▪ Information on income and credit ratings
Transactional data	▪ History of purchases via loyalty cards, completed online and/or prices paid ▪
Contact information	▪ Individual's home/work address ▪ Email address ▪ Phone number
Socio-demographic data	▪ Age ▪ Ethnicity ▪ Gender ▪ Level of education ▪ Occupation and social class (e.g. sector, net worth associated with a specific profession) ▪ Household Income ▪ Number of family members (e.g. number, gender and age of children) ▪ Religion
Contractual data	▪ History from utility suppliers, contract service details
Location data	▪ Mobile devices ▪ Vehicle telematics ▪ GPS data and history of/planned journeys entered into the satellite navigation system ▪ Sensor data (from radio-frequency identification (RFID)
Behavioural and interests' data	▪ History of visited websites and clicks on advertisements (which could include searches on sensitive topics such as health problems or political views) ▪ Games and applications used ▪ Telematics data from automotive insurance companies ▪ Posts on social media, professional websites and blogs ▪ Email exchanges
Technical data	▪ IP address ▪ Data related to the device (e.g. type, international mobile equipment identity (IMEI)) ▪ Browser information

One of main objectives of the General Data Protection Regulation (GDPR) is to protect the fundamental rights and freedoms of natural persons, and their right to the protection of personal data. The level of safeguarding corresponds to the level of privacy risk associated to the different typologies of data:

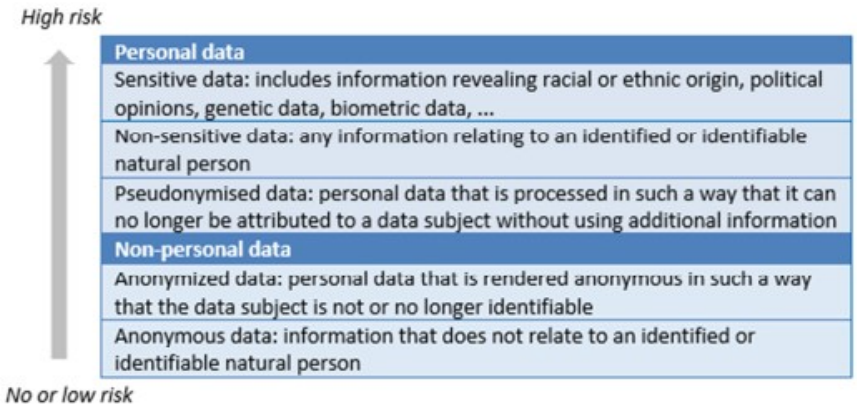


Figure 2: Typology of data with the associated data protection risk[15]

As such, the typology is not directly related to the specifi economic value of the data. Certain types of non-personal data might be more valuable than personal data, but only the latter, when processed, is

[15] De Streel A., Bourreau M., Graef I., (2017), Big Data and Competition Policy: Market power, personalised pricing and advertising, CERRE, pag.15

subject to the requirements of EU data protection legislation. Big data analytics may bring higher productivity or efficiency, even without the collection or use of personal data.

Furthermore, the typology is not equivalent to a market definition as performed under competition law. A relevant upstream, intermediate or downstream market for data may include personal as well as non-personal data depending on the circumstances. The definition of a relevant market for data is complex and requires the competition authority to assess substitutability between different kind of data. This is beyond our purpose at the moment, we will instead approach the issue in the third section of our work[16]. There, we analyse how agencies defined the relevant market of two different cases where personal data is a crucial parameter of competition. We will also propose a conceptualization of personal data as "non-monetary price", which have some relevant implications in terms of market definition tools. Now, instead we focus on the different categories of personal data and on the legal constraints applicable to their collection and use.

2.2 Identifiability and sub-categories of personal data

We saw above that the key in the definition of personal data is the concept of "identifiability"[17].To determine whether a natural person is identifiable, attention should be paid to the means likely to be used either by the controller or by any other person to identify the said person. Additional guidance on how to interpret the concept of identifiability was given by the Article 29 Working Party[18] and codified in the General Data Protection Regulation, which states that (Recital 26): '*account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments*'.

Typology of data and the associated data protection risk

The different types of personal data are subject to different levels of protection under EU data protection law (in Figure 2 above). Apart from the main distinction between personal and non-personal, there are other sub-categories. We will now see more in the detail the features of sensitive, pseudonymised, anonymous data and anonymized ones.

Sensitive data

Sensitive data are those to which stricter rules are applied. They are a special category of personal data, which includes information revealing racial or ethnic origin, political opinions, health, religious or

[16] See Section III - The Intersection between Competition Law and Data protection, p.43

[17] The key notion of personal data is defined as '*any information relating to an identified or identifiable natural person (data subject)*'. An identifiable natural person is, in turn, defined as 'one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person'. These are the definitions contained in Article 4(1) of the General Data Protection Regulation.

[18] The Article 29 Working Party was set up under Article 29 of the Data Protection Directive and is composed of a representative from the national data protection authority of each EU Member State, a representative of the European Data Protection Supervisor (the independent supervisory authority that is responsible for ensuring that all EU institutions and bodies respect people's right to personal data protection and privacy when processing their personal data) and a representative of the European Commission.

philosophical beliefs, trade union membership, person's sex life or sex orientation, and the processing of genetic and biometric data for the purpose of uniquely identifying a natural person. Processing of this type of information is prohibited unless one of the lawful grounds of processing listed in EU rules applies. It has been showed[19] that companies indeed collect sensitive data on topics such as health, political views or sexual orientation for online targeted advertising. An article published by the *Economist* in 2014[20] showed the evidence of companies applying targeted advertisement based on personal health data, although many advertisers claim not to have interest in sensitive data.

Data which is not sensitive in itself, may become such when integrated with other information available on the consumer. Why do companies collect these kinds of sensitive data, despite the prohibition under the European data protection framework? The main reason is that sensitive data is more valuable on the data market: providing highly detailed information and allowing to better target consumers[21]. The purpose of personalisation is, in fact, to segment users rather than to reveal their individual identity[22].

Pseudonymised data

Pseudonymised data is personal data processed in in a way that 'it can no longer be attributed to a specific subject without additional information, provided that such additional information is kept separately and is subject to technical measures to ensure that the personal data are not attribute to an identified or identifiable natural person'[23]. Since pseudonymised data may still identify a natural person, it is considered as personal data to which the data protection rules fully apply[24].

Subcategories of non-personal data

Non-personal data is information that is not protected under data protection law. A distinction can be made between anonymous and anonymised data.

Anonymous data is information which does not relate to an identified or identifiable natural person (taking account of all the means available to the controller or to any other person for the identification). An example of anonymous data is machine data created by the activity of computers, mobile phones and other systems or devices. However, even these data may considered as personal

[19] European Commission Report, Consumer market study on online market segmentation through personalised pricing/offers in the European Union final report, 2018, p.52

[20] The Economist, "Getting to know you", September 2014. Available at: http://www.economist.com/news/special-report/21615871-everything-people-do-online-avidly-followed-advertisers-and-third-party

[21] Emily Steel, Financial Times, "*Financial worth of personal data comes in under a penny a piece*". Article. 12 June 2013. https://www.ft.com/content/3cb056c6-d343-11e2-b3ff-00144feab7de

[22] The UK Office of Fair Trading (OFT) identified in 2013 a general trend related to personalised pricing: businesses are more interested in identifying *"different sorts of customers and segment their customer base into fine groups, rather than seeking to identify who individuals are".*

[23] Article 4(5) of the General Data Protection Regulation. An example of pseudonymisation is key-coded data used for statistical or scientific purposes. Key-coded data is information relating to a data subject who is earmarked by way of a code that is not derived from information identifying the individual. The key making the correspondence between the code and the common identifiers of the individual (such as name, address, date of birth) is kept separately. This way, taking into account all the means reasonably likely to be used, it is possible only to trace the information back to the data subject by referencing the key.

[24]Recital 26 of the General Data Protection Regulation

data where information is collected about the behaviour of an identifiable natural person, such as call detail records generated by telephony systems and search logs generated by online search engines.

Anonymised data, instead, is personal data which is rendered anonymous in a manner that the data subject is no longer identifiable[25]. In the case of anonymised data the identification is no longer possible. If the anonymisation is irreversible[26], there is no application of the EU data protection rules.

Although anonymisation, and to a lesser extent pseudonymisation, reduce the privacy risks for consumers, these techniques still do not fully guarantee data protection. The distinction between personal and non-personal data becomes less clear if pseudonymisation and anonymisation techniques are not applied properly, as they can be reversed to allow to identify the individual. A report by Cracked Labs indicated that companies tend to use data which is pseudonymous rather than anonymous[27]. As we have seen, the main difference between "anonymization" and "pseudonymisation" is the possibility of re-identification of the data subject. Pseudonymisation offers more limited privacy protection than anonymisation and it still allows for the indirect identification of individuals. As noted in an Article 29 Data Protection Working Party Opinion, it only reduces the "linkability" of a dataset with the original identity of a data subject, without being a method of anonymization. Anonymisation prevent the re-identification of the individual even in cases of aggregating and combining information obtained from different sources. However, it could still entail privacy risks for consumers. Its efficiency depends on its appropriate engineered application[28].

The Article 29 WP Opinion states that properly anonymised datasets should not allow companies to re-identify individuals by: (i) **Singling out:** isolating the records of an individual in a dataset; (ii) **Linkability:** linking two records concerning the same data subject, or a group of data subjects, in the same of different datasets; (iii) **Inference:** the possibility to deduce with significant probability, the value of an attribute from the values of a set of other attributes

Therefore, the Opinion states that "as long as the data is identifiable, data protection rules apply", and warns against adopting pseudonymous and anonymous techniques interchangeably[29]. Furthermore, claims of anonymity can be misleading since datasets can be de-anonymised by combining information from different sources and linking anonymous data with personally identifiable information (e.g. name, address)[30].

While the findings from the literature as well as the business operators consulted for the European Commission report[31] suggest that companies usually remove the names collected on individuals and encrypt other personal identifiers, these hidden identifiers can still be linked across other online services and databases and matched to a profile[32]. Individuals' names are not the only interesting

[25] Recital 26 of the General Data Protection Regulation. Also, Opinion 4/2007 of the Article 29 Working Party of 20 June 2007 on the concept of personal data, WP 136, p. 21
[26] Article 29 Working Party, 'Opinion 05/2014 on Anonymisation Techniques', WP 216, 10 April 2014.
[27] Wolfie C., Cracked Labs (2017), "Corporate surveillance in everyday life: How companies collect, combine, analyse, trade, and use personal data on billions".
http://crackedlabs.org/dl/CrackedLabs_Christl_CorporateSurveillance.pdf
[28] Opinion 05/2014 referenced above.
[29] Idem
[30] Rao et Al. referenced above
[31] European Commission Report, Consumer market study on online market segmentation through personalised pricing/offers in the European Union final report, 2018
[32] Idem

parameter for the re-identification of a person. Earlier studies showed that combining the date of birth, gender and zip code is enough to identify an individual: for example, such kind of information allowed for the unique identification of 87% of the United States population (216 million of 248 million in 2000)[33]. Identification was even possible with less precise identifiers (e.g. city or country), in combination with birthdate and gender[34]. In addition, retailers can combine zip codes with information captured at stores' points-of-sale (e.g. name, telephone number, credit card details) to determine the home address of the individual[35].

Conclusion

In this first chapter we have tried to define more deeply what are personal data, which will be the core of our discussion around privacy and competition law. Until now, we presented the legal definition of personal data and the European Union legal framework under which they are treated. The discussion will be useful again in the third section of the work. In the next chapters, we will focus more on the economic and competitive dimension of personal data. We will see what is their role in data-driven business models, and which are the features that make them so important and valuable for several types of online services and platforms.

3. Big personal data as an asset

Companies across all sectors of the economy rely on enormous volumes of an innvative intangible asset: personal data. Extracting value from big data has become a significant source of power for the biggest players in internet markets. Not all big data is personal, but for many online products which are presented as being 'free', personal information is indeed a sort of currency paid by users. Consumers provide this important input for digital economy daily. In return, they are able to access to services that would otherwise require a monetary fee[36]. For consumers, therefore, personal information operates as a currency, and sometimes it is the only currency to have access to online services[37]. Commissioner Vestager once stated: "We're living at a time when technology is transforming our world; intelligent algorithms, working with huge amounts of data are changing every

[33] Latanya Sweeney, Simple Demographics Often Identify People Uniquely. Carnegie Mellon University, Data Privacy Working Paper 3, Pittsburgh 2000. Available at: https://dataprivacylab.org/projects/identifiability/paper1.pdf

[34] Idem

[35] Adam Tanner, Forbes (2013), "Never Give Stores your zip code. Here's why". Available at: https://www.forbes.com/sites/adamtanner/2013/06/19/theres-a-billion-reasons-not-to-give-stores-yourzip-code-ever/#70291b6c786f.
See also: Chris Jay Hoofnagle, Behavioural Advertising: The Offer you can't refuse, 6 Harv.L.& Pol'y Rev.273(2012). Available at: http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=3086&context=facpubs

[36] Magali E., Market Definition and Free Online Services: The Prospect of Personal Data as Price (July 3, 2018). I/S: A Journal of Law and Policy for the Information Society, Vol.14:2 (2018) 227. P.229

[37] 'Personal data is the currency of today's digital market;' speech by Vice Commissioner Reding, 'The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age – Innovation Conference Digital, Life, Design', Munich, 22 January 2012

part of the way we live."[38] Yet, the companies offering these services are not charities, they are out to make a profit and the value extracted from big data has become a significant source of power for the biggest players in internet markets. As well as benefits, these growing markets pose specific risks to consumer welfare and to the rights to privacy and data protection. They also raise competitive concerns, as we will try to show along all our work.

The digital economy is marked by strong, dynamic growth, a high turnover of new services, market concentration involving few dominant players, and a great imbalance between big companies on the one side, and SMEs and individual users on the other side. This growth is fundamentally based, in many sectors of the economy, on advances in data mining and analytics and on the availability of impressive computing power and data storage capacity. Masses of personal information are generated by over 460 million internet users in the EU28 through their consumption of social media, games, search engines, e-commerce and other services. Information collected on subscribers to given online services include names, gender, personal preferences, location, email addresses, IP addresses and surfing history. Whereas data had been previously gathered as a secondary part of the transaction, the added value of big data derives especially from the potential correlations uncovered by data analytics, which can open the way for uses which have nothing to do with the original purposes for which data was collected[39]. Estimates of this added value vary according to context and methodology: the net income per record/user for two global companies whose business models is pivoted on personal data have been calculated at EUR 3-5 per year[40]; while the digital value that EU consumers place on their data was estimated at EUR 315 billion in 2011, forecasted to rise to EUR 1 trillion by 2020[41].

The extent to which companies should be able to monetise the personal datasets acquired has been the subject of huge debate. We will see further in the text which are the relevant issues animating scholars, enforcers and the various institutions. Nevertheless, personal information has become a substantial intangible asset used for the purposes of value creation, comparable to copyright, patents and intellectual capital[42]. Often it is a company's most valuable asset.

4. The four 'V's: Volume, Variety, Velocity and Value

To better understand the competitive potential of personal data, we need to understand four features which are very well known nowadays and that characterise the online environment. These features are not strictly specific to personal data, they are common to all kind of Big Data, non-personal ones included. These features have generally been categorized in the literature as four 'V's: namely, the

[38] Speech by M. Vestager - European Commissioner for Competition, *Setting innovation free*. Bpifrance Inno Génération: Paris 2017

[39] Moerel L., inaugural address Tilburg Law School, 'Big Data Protection: How to Make the Draft EU Regulation on Data Protection Future Proof', 14.02.2014.

[40] See OECD (2013), Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value, OECD Digital Economy Papers, No. 220, OECD Publishing. The announced acquisition of WhatsApp by Facebook for USD 19 billion was the equivalent of paying EUR 30 for each of the messaging service's 450 million users.

[41] Boston Consulting Group, *The Value of our Digital Identity*, November 2012

[42] This has been recognised by the Commission several times in the past: 'Today, personal data are a type of asset for companies' (speech by Vice-President Almunia, 'Competition and personal data protection', 26 November 2012); '…big data is not just a new sector, but a new asset class. One that sits as a pillar of our economy, like human resources or financial capital' (speech by Vice-President Kroes, Big Data for Europe, 7.11.2013).

volume of data; the *velocity* at which data is collected, used, and disseminated; the *variety* of information aggregated; and finally, the *value* of the data. Each 'V' has increased significantly over the past decade. Let see how these four V's apply to personal data.

4.1 Volume of Data

The volume of data collected has increased significantly and continues to grow. The firm Cisco forecasted the growth of global data centre IP traffic and predicted that the annual global data centre IP traffic would have reached 8.6 zettabytes by the end of 2018, up from 3.1 zettabytes in 2013.[43] This is an old forecast, but we need it to better comprehend the dimensions of the matter we are discussing. To put 8.6 zettabytes in perspective, if every person in the world (7,211,239,210 in 2014) were to store some of the 8.6 zettabytes data on an iPhone 6 (the largest at the time with 128 gigabytes storage), that would had required over ten iPhones per person (10.24420843 to be exact) or 73,873,437,491 iPhones in total[44]. As the OECD noted: the digitisation of nearly all media and the increasing migration of social and economic activities to the Internet (through e-services such as social networks, e-commerce, e-health and e-government) are generating petabytes (millions of gigabytes) of data every second.[45]

One reason for the increase in data collection is the decrease in cost to collect, store, process, and analyse it. Moreover, with the rise of broadband access, smartphones, e-commerce, and social networks, consumers are actively and passively divulging more personal information. To matter is not only the absolute volume of data, but the volume relative to a comprehensive dataset on a certain topic. Social networking is one striking example in this sense. In 2014, the OECD noted that there were 'over 900 million active [Facebook] participants around the world' who 'generate on average more than 1500 status updates every second'.[46] As the Executive Office of the US President observed, 'the volume of information that people create themselves—the full range of communications from voice calls, emails and texts to uploaded pictures, video, and music—pales in comparison to the amount of digital information created about them each day'.[47] Today, Facebook have over 2.41 billion monthly active users (MAU) worldwide, as of June 2019.

With the Internet of Things, sensors, microphones, and cameras are going to provide even more data about us, tracking us in our homes, cars, schools, at work, or during free time. One's data trail begins before one's birth, with retailers - like Target - using data analytics to identify and target pregnant shoppers with coupons,[48] and increases until one's death.

[43] Cisco, *Cisco Global Cloud Index: Forecast and Methodology, 2013–2018'* (2014).
[44] Stucke M.E. & Grunes A.P., (2016), *Big Data and Competition Policy*, Oxford University Press, p.17
[45] OECD, *Data-Driven Innovation for Growth and Well-Being: Interim Synthesis Report*, October 2014, http://www.oecd.org/sti/inno/data-driven-innovation-interim-synthesis.pdf
[46] Idem
[47] The Executive Office of the President, *Big Data: Seizing Opportunities, Preserving Values*, May 2014, p. 2 ('White House Big Data Report').
[48]Duhigg C., 'How Companies Learn Your Secrets', *NY Times*, 16 February 2012.

4.2 Velocity of Data

The velocity at which data are generated, accessed, processed, and analysed has also increased, and for some applications is approaching real-time. Consequently, there is a 'growing potential for big data analytics to have an immediate effect on a person's surrounding environment or decisions'[49]. We see this with automated stock trading and other machine learning, where autonomous systems, through algorithms, can learn from data of previous situations and make autonomous decisions. Companies mine their data 'to make real-time "nowcasts"[50] in order to improve the quality of policy and business decisions. That is way to be the first to access data can confer a robust competitive advantage. For example, messaging apps and social networks, which are currently at the core of our discussion, really collect and analyse information about users in real time. A text conversation in a messaging online service can provide instantaneous information about the current activity or plans of a user: going to the restaurant, organizing a trip, asking some advices on some products.

The velocity in processing data will likely increase in other fields which are now considered to be the next innovative revolution, such as driverless cars and Internet of Things. The value of data is closely related to this velocity dimension; depending on the purposes, older data may be less valuable than more recent ones. Current geo-location data, for example, may be very important for the commuter in choosing which roads are less congested, while historic traffic data is less useful for this purpose.

4.3 Variety of Data

Data's value increases not only with its volume and the velocity in processing practices, but also with the variety of information collected on an individual.

A great example can be the dataset collected by the UK retailer Tesco on its customers[51]. The chain store of supermarket gathers a huge amount of information from its loyalty programme. It then collects the shopper's purchase history and visit history, both to stores and online, which allow to identify customer's preferences and tastes. Finally, Tesco mines other databases to further develop its shopper profile, including 'credit reports, loan applications, magazine subscription lists, Office for National Statistics, and the Land Registry'.[52] Why do firms collect such variety of personal data? As Tesco former CEO Terence Patrick Leahy noted 'We could treat customers as individuals. And we could learn what they were interested in, what their behaviours were, and we could tailor and target all of their marketing so that it was relevant to that individual consumer.'[53]

---

[49] The Executive Office of the President, *Big Data: Seizing Opportunities, Preserving Values*, May 2014, p.5 ('White House Big Data Report').

[50] One example of the velocity of data is 'nowcasting', which Google's Chief Economist defined as "contemporaneous forecasting"—basically an ability to predict what is happening as it occurs. See: Auction.com, 'Auction.com Launches Real Estate's First Nowcast—Leverages Industry, Transactional and Google Search Data to Provide Accurate Real-Time Market Intelligence', Press Release, 30 October 2014

[51] The example is reported by Stucke M.E. & Grunes A.P., (2016), *Big Data and Competition Policy*, Oxford University Press

[52] Krish Swarmy, 'Analyzing Tesco—The Analytics Behind a Top-Notch Loyalty Programme', *Big Data Analytics*, 21 August 2011, http://stat-exchange.blogspot.com/2011/08/analyzing-tescoanalytics-behind-top.html

[53] Brad Howarth, 'How Tesco's loyalty card transformed customer data tracking', *CMO*, 21 May 2015, http://www.cmo.com.au/article/575497/how-tesco-loyalty-card-transformedcustomer-data-tracking/.

As this example illustrates, data's value increases through data fusion, which links data from different sources and makes new correlation emerge. In this way, companies can identify and improve their profiles of individuals, better track their activities, preferences, and vulnerabilities, and better target them with behavioural advertising. These detailed personal profiles and personalized experiences are effective in the consumer marketplace and make efficient the delivery of products and offers to precise segments of the consumers population.[54]

4.4 Value of Data

The volume and variety of data being collected and the velocity in processing the data have increased because of data's value. Big Data is tied to big analytics, from which data's value is derived. Data analytics are defined as 'the technical means to extract insights and the empowering tools to better understand, influence or control the data objects of these insights (e.g. natural phenomena, social systems, individuals)'.[55]Big Data and Big Analytics mutually reinforce each other. Big Data are less valuable if companies can't quickly analyse them and act upon it. Machine-learning, in turn, relies on accessing large data sets. As the European Data Protection Supervisor observed, 'deep learning computers teach themselves tasks by crunching large data sets using (among other things) neural networks that appear to emulate the brain.'[56] The algorithms' capacity to learn increases with the amount and relevance of data available.

Here we see how Big Data's value derives from the other three 'V's. The volume of data can enable firms to uncover correlations from large, unprocessed datasets, which can outperform findings from smaller, but cleaner datasets. Value comes from the variety of data and their fusion. Finally, value comes from velocity, namely being the first to collect, analyse, and use the data. With real-time monitoring and self-learning computer algorithms automatically updating their inferences, companies can be the first to predict material changes in the market.

Conclusion

Volume, variety, velocity and value: these are the basic features common to all kind of data, personal and non-personal ones. However, it is already evident how social networks and messaging apps (or more generally "social media") really bring the V's potential to the maximum limit. Nowadays, a Facebook user's profile provides a 360-degree portrait on his thoughts, interests, activities, friends, and this tracking doesn't stop to Facebook. It works also on the other owned services: WhatsApp and Instagram, Masquerade and Oculus, adding more variety and specificity to the profile. The tracking goes on while surfing on third-party website too, even when users are not actually active on Facebook platforms (this is the central issue of the Bundeskartellamt investigation that we will analyse in section III). Volume, Velocity, Variety become, at the end, Value: biggest share of Facebook's profits derives from advertising and from the very high level of targeted ads offered by the company.

[54] White House Big Data Report, supra, p. 7.
[55] OECD, *Data-Driven Innovation*, supra, p. 4.
[56] European Data Protection Supervisor, 'Towards a New Digital Ethics: Data, Dignity and Technology', Opinion 4/2015, 11 September 2015

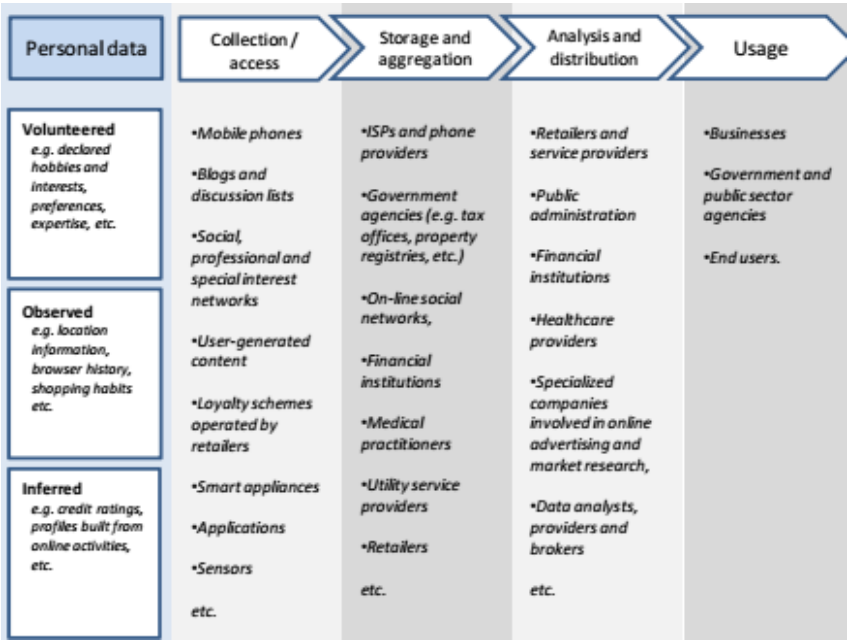
in the next chapter, we put together all those elements necessary to understand the competitive importance of personal data in the digital world. In order to find out how a dataset finally acquires his value and becomes a source ready to be employed, we describe the "data value chain" at the basis of all data-driven technologies and services.

5. The personal data economy: Mapping value chains and business models

The consumer data 'value chain' is the chain by which consumer data is generated, collected and processed commercially to create value. A four-step chain has been identified and explained by OECD (2013)[57], consisting of: (i) collection and access; (ii) storage and aggregation; (iii) analysis and distribution; (iv) usage of personal datasets. A multiplicity of individuals, businesses, public institutions and non-profit organisations take part to this value chain.

Personal data is collected in a variety of ways[58]: data can be **volunteered or surrendered**, when individual explicitly share information about themselves or about third parties (e.g., creating a social network profile, entering credit card information or posting information about friends, family members and colleagues); data can be **observed** by recording individuals' activities online (e.g., Internet browsing preferences, mobile phone geo-localization); and finally data can be **inferred** through the analysis of personal information (i.e., credit scores can be calculated based on a number of factors relevant to an individual's financial history). Personal data can be also *inferred* from several pieces of seemingly anonymous data.

Figure 3: Data value chain[59]



[57] Organisation for Economic Cooperation and Development (OECD), 'Exploring the Economics of Personal Data', 2013

[58] Ibid. p.10

[59] OECD (2013), Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value, OECD Digital Economy Papers, No. 220, OECD Publishing, p.11

5.1 Collection / access

The collection or access step in the value chain has been radically transformed by the growth of the Internet and other communication technologies. Nowadays, economic players like mobile network and Internet service providers have access to highly detailed information on consumers. However, even in non-ICT sectors, retailers have acquired better tools to track sales to customers, using loyalty cards and even in-store tracking technologies. Generally, data can be collected directly or indirectly. Online direct data collection is typically done in different ways: data can be publicly observed (through devices, IP addres, operating system); voluntarily provided (information entered to register to services and to log-in websites); or acquired by tracking users[60].

In some cases, data is gathered indirectly, which is related to the emergence of newer business models. Firms may procure data from third-parties and intermediaries. On the basis of a business models survey done by Deloitte, the European Commission observes that: "in the vast majority of cases (78% of the companies surveyed) data is generated and analysed in-house by the company or by a sub-contractor. Vertical integration remains the principal strategy in the sectors surveyed. Data stays within an organisation and is not traded with third parties."[61] According to this study, in Europe data trading remains a marginal practice, accounting only for 4% of the companies surveyed. In this case, data can be obtained from data brokers[62] on the data marketplace.

Data marketplaces in their simplest form are online stores where firms can buy and sell data[63]. On this secondary market, data from multiple offline and online sources are traded between different data brokers. A 2014 FTC report found some of the biggest data brokers in the US to be in possession on an impressive amount of personal data on almost every US household and commercial transaction.[64]

5.2 Storage and aggregation

Once data has been collected, it is stored and aggregated. This is the second stage of the value chain. The individual data elements are organised and stored in datasets and used for further processing and

[60] Here some tools used: tracking cookies, history sniffing, device fingerprinting, cross-device tracking. For a more detailed explanation, see: De Streel A., Bourreau M., Graef I., (2017), *Big Data and Competition Policy: Market power, personalised pricing and advertising*, CERRE, p.13

[61] Commission Staff Working Document of 10 January 2017 on the free flow of data and emerging issues of the European data economy, SWD(2017) 2, p. 15.

[62] US Federal Trade Commission, Data Brokers: A Call for Transparency and Accountability, 2014 defined data brokers as 'companies whose primary business is collecting personal information about consumers from a variety of sources and aggregating, analysing, and sharing that information, or information derived from it, for purposes such as marketing products, verifying an individual's identity, or detecting fraud'.

[63] The consultancy IDC (2016) defined a broad concept of data marketplace as "a third party, cloud-based software platform providing Internet access to a disparate set of external data sources for use in IT systems by business, government or non-profit organizations. The marketplace operator will manage payment mechanisms to reimburse each dataset owner/provider for data use, as necessary. Optionally, the marketplace provider may provide access to analysis tools that can operate on the data."

[64] This report (quotes above note 62) reported data brokers hold a vast array of information on individual consumers. For example, one of the nine data brokers examined had 3000 data segments for nearly every U.S. consumer. Based on companies' reports, Lambrecht and Tucker (2015:5) note that: Acxiom has multi-sourced insight into approximately 700 million consumers worldwide with over 1,600 pieces of separate data on each consumer; Datalogix asserts that its data includes almost every U.S. household; Bluekai states that it has data on 750 million unique users per month with an average of 10-15 attributes per user.

analysis. Numerous personal data records such as contact and credit card details, account and login authentication details are stored by a wide range of services providers such as ISPs and phone providers, retailers, transportation firms, medical practitioners, utilities and government agencies, by service and content providers, like social and professional networks, blogs, photo and video sharing sites. Data is also aggregated and stored by various public and private sector agencies like banks, employers and taxation agencies, healthcare insurers.

5.3 Analysis and distribution

The third step in the personal data value chain is the combination of collected and stored data with other information to develop detailed profiles, records, and macro trends used for various purposes[65]. Analytics is used to infer information that may not be otherwise available. The sources of data may include data sets publicly available, proprietary data owned by businesses, and data from institutional research[66]. Data are subject to several rounds of analysis and distribution, where other additional data are processed. The insights are used to have more refined personal profiles and data analytics firms often resell the combined profiles in the market.

Examples of other types of insights drawn from such analyses include improved customer service and product quality, drug interaction issues, and common daily traffic patterns. This work is often done by firms with developed infrastructure, strong analytical skills and developed distribution networks. This can involve both traditional players and new firms that have emerged in response to more recent needs and opportunities. For instance, the former are usually retailers and service providers of customer relationship management (CRM) softwares, business intelligence systems and loyalty programmes. The recent players are usually involved in online advertising, market research, specialised data analysts and brokers[67].

The distribution of the processed information takes many forms. Major players generally use the data they collected and processed. Others trade the data they collect and some purchase processed data as a service from data analysts and brokers and/or on data exchanges. In online advertising, a data exchange is a marketplace where advertisers bid for access to data about customers.

5.4 Usage

Once the data have been collected, stored and analysed, they become available to the end users of the value chain. The end users generally purchase profiles of individuals (or firms) in order to supplement their own business activities. Personal data are used in many ways by businesses, public sector agencies and end users. Personal data are typically used to better understand customers, to offer them targeted ads and improve the efficiency of transactions between the entity and end-users. They can be used to improve business operations, as well as to identify macro trends in different sectors, like healthcare, transportation, and safety.

[65] OECD (2013), *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD Digital Economy Papers, No. 220, OECD Publishing, p. 13
[66] Ibid.
[67] Ibid.

Governments increasingly rely on personal data, obtained not only from third parties but also directly from individuals, to administer various programmes. Examples include social service programmes, tax programmes or issuing licenses. Data is commonly used to support regulatory regimes like voter registration, disclosure of political campaign contributor, employee identity verification and child support obligation enforcement. Other uses can be to maintain vital records about major lifecycle events, including birth, marriage, divorce, adoption, and death; or to operate facilities such as toll roads and national parks. Personal data helps to provide services to a larger population, diminishes the perceived inequality of subjective determinations, reduces the costs of litigating decisions and maintaining more skilled personnel, and enhances accountability[68].

6. The competitive value of personal data: an intangible asset

In the previous chapters, we have seen which are the digital and technological elements which make big data, and personal data, so crucial and valuable for data-driven products and services. We presented briefly the four-step value chain upon which all these business models are pivoted and organised: the collection, storage, analysis and usage. Now, it is time to consider these practices from a proper competition law perspective. We will highlight which are the competitive strategies and advantages related to big data. In particular, we will see how entry barriers, network effects, economies of scale and scope can occur in these data-driven environments and how these competitive factors can be sometimes different and more difficult to tackle for authorities. As for the previous analysis, the issue we are going to present are not in themselves specific to personal data but are anyway strictly applicable to them and furthermore important to prepare our last discussion about the intersection between competition law and privacy law.

6.1 Looking beyond traditional entry barriers

Apart from per se illegal antitrust offences, like price-fixing, antitrust analysis generally considers the ease of entry. Companies cannot exercise market power for long when entry from competitors is timely (generally under two years), likely (profitable for the entrants), and sufficient (the entrants would attain sufficient business to prevent the exercise of market power by the incumbent firms).[69] It is a common opinion that online markets are characterized by low entry barriers and typically do not require big data for entry. For example, the chairman of Google, one of the world's largest collectors of personal data stated that 'the barriers to entry are negligible, because competition is just one click away'[70] and 'Our experience is that you don't need data to compete online.'[71] The reality is that there is no empirical support for concluding that entry barriers are invariably low or high across online markets. The entry analysis for data-driven markets is fact-specific. Some argue that data does not lend

[68] Cate, F. H., (2008), Government Data Mining: The Need for a Legal Framework, *Harvard Civil Rights-Civil Liberties Law Review*. 43, 2008

[69] US Department of Justice (DOJ) and Federal Trade Commission (FTC), *Horizontal Merger Guidelines*, 19 August 2010, s 9, https://www.ftc.gov/sites/default/fles/attachments/merger-review/100819hmg.pdf

[70] Eric Schmidt, Executive Chairman of Google, 'Why Google Works', *Huffington Post*, 20 January 2015, http://www.hufngtonpost.com/eric-schmidt/why-google-works_b_6502132.html.

[71] Eric Schmidt, Executive Chairman of Google, 'The New Gründergeist', *Google Europe Blog*, 13 October 2014, http://googlepolicyeurope.blogspot.com/2014/10/the-new-grundergeist.html.

itself to entry barriers, and in certain contexts this is true. Under the traditional factors generally considered by agencies, entry barriers may seem low, excluding the need for an intervention: online industries are dynamic, fast-growing and highly innovative, the products and services provided are often free on the consumer side, and finally the digital market does not exhibit high switching costs for consumers.

What we want to remark here is that firms can have market power even once considered all these facts mentioned above. Observing the products or service which are supplied free of charge, we have a first proof of that. Companies, like Facebook and Google, have tremendous market power for free products, and "zero-price" might even be *supra*-competitive whenever a competitive market offers a negative price (i.e., the company pays you to toil on its social network providing information to attract others' users). Moreover, digital platforms and services also differ in terms of network effects, going beyond the direct ones traditionally identified by the courts and agencies[72]. We will analyse better this intuition later in the chapter. Competition authorities will have a distorted picture of the market if they consider only the traditional entry barriers and traditional network effects. They must care about additional data-driven network effects, which can lead to market concentration and dominance.

6.2 Dataset and market power

According to the joint report by Autorité de la concurrence and the Bundeskartellamt[73], there are two main factors to assess when the control of a dataset is a source of market power: (i) the scarcity of data (or ease of replicability) and (ii) whether the scale/scope of data collection matters to competitive performance.

The CERRE (Centre of Regulation in Europe) report entitled 'Big Data and Competition Policy: Market power, personalised pricing and advertising[74]' remarks that this assessment should be done on a case-by-case basis and it depends significantly on the type of data and the type of use of such data. Very important is to analyse carefully the different steps of the data value chain: in steps like data collection and data analysis, because of potential non-replicability, the risks of entry barriers are a-priori higher than for data storage. In the next paragraphs, we will follow the guidelines set by the CERRE report and treat the various phases of the value chain.

6.2.1 Data collection

One intrinsic characteristic of data is the non-rivalry, meaning that the same data can be collected and used many times without losing value. Ceteris paribus, this feature impacts directly on the costs of collection by firms. However, there may still be some technical, legal or contractual conditions able to

[72] If this were true, then the low entry barriers and switching costs should prevent any search engine from intentionally degrading quality (in terms of the relevance of the response to a search inquiry). As the European Commission's statement of objections involving Google reflects, that is not the case. See European Commission, 'Fact Sheet: Commission Sends Statement of Objections to Google on Comparison Shopping Service', 15 April 2015, http://europa.eu/rapid/press-release_MEMO-15-4781_en.html

[73] Autorité de la concurrence and Bundeskartellamt, (2016), *Competition law and data*

[74] De Streel A., Bourreau M., Graef I., (2017), *Big Data and Competition Policy: Market power, personalised pricing and advertising*, CERRE, p.30

humper the non-rivalry of a dataset, making it exclusive.[75] Legal barriers especially increase the costs of collection, as we will see better in Section III. This is particularly the case for personal data whose means of collection are limited by the general data protection rules (GDPR).

In some cases, data are collected for their own sake and the collecting firm invests only for the purpose of gathering data. This business model is generally more affected by network and experience effects than the traditional model and it may lead to large platforms offering supposedly free services and collecting huge amounts of personal data[76]. In other cases, data are collected as by-product of the commercial activity of the firm, which does not invest specifically with the purpose of collecting data. This data collection as by-product increased with the proliferation of connected devices and the diminishing costs of information storage. The cost of collection is obviously higher in the first business model than the second one. Of course, those above-mentioned are two extreme cases and reality usually lies in-between. For example, there are cases where investments in improving products are made in order to get better data as by-products.

6.2.2 Antitrust assessment of data availability and replicability

In several cases, availability and collection costs have been an important criterion for competition agencies in assessing whether a dataset was replicable or not. In some merger cases involving big data-driven online firms, the Commission concluded that datasets of the merging parties were replicable and the combination of those data would have not impeded significantly competition. In the Google/DoubleClick, Facebook/WhatsApp and Microsoft/LinkedIn investigations, the Commission considered that the combination of the datasets post-mergers was not creating competitive foreclosure, since a large amount of data sources would have remained available to competitors[77]. However, in other abuse of dominance cases, some national competition authorities decided that datasets gathered by firms enjoying a legal monopoly might not be reproducible by competitors and couldn't be used to launch other rival services: in September 2014, the *Autorité de la Concurrence* adopted an interim decision in which GDF Suez was found capable of taking advantage of its dominant position in the market for natural gas by using the customer files inherited from its former monopoly status. The French agency considered that it was not possible for the competitors to reproduce this advantage or to rely on other alternative databases.[78] In 2015, a similar decision was taken by the Belgian Competition authority on the Belgian National Lottery[79]: the data owned by the former

[75] Graef I., (2016), EU Competition Law, *Data Protection and Online Platforms: Data as Essential Facility*, Kluwer Law International

[76] Autorité de la Concurrence and Bundeskartellamt, (2016), *Competition Law and Big Data*, p.38

[77] Commission Decision of 11 March 2008, Case M.4731 *Google/ DoubleClick*, para. 364-366; Commission Decision of 3 October 2014, Case M.7217 *Facebook/WhatsApp*, para. 167-189. Commission Decision of 6 December 2016, Case M. 8124 *Microsoft/LinkedIn*.

[77]Commission Decision of 3 October 2014, Case M.7217 *Facebook/WhatsApp*, para. 167-189.

[77] Commission Decision of 6 December 2016, Case M. 8124 *Microsoft/LinkedIn*.

[78] Autorité de la concurrence, Décision 14-MC-02 du 9 septembre 2014 relative à une demande de mesures conservatoires présentée par la société Direct Energie dans les secteurs du gaz et de l'électricité, par. 147-154.

[79] [79] Belgian Competition Authority, Beslissing BMA-2015-P/K-27-AUD van 22 september 2015, Zaken nr. MEDE-P/K- 13/0012 en CONC-P/K-13/0013, *Stanleybet Belgium NV/Stanley International Betting Ltd en Sagevas S.A./World Football Association S.P.R.L./Samenwerkende Nevenmaatschappij Belgische PMU S.C.R.L. t. Nationale Loterij NV*, par.44-48.

Monopoly were not considered to be replicable and available to other rivals in the market of sports betting[80].

6.3 Data analysis

The volume, variety and velocity of data deeply impact the value and quality of the information inferred from the datasets. The relationship between these four V's obviously depends on the type of data collected and on type of analysis performed. Data analysis is the moment in which we can observe economies of scale and scope deriving from the accumulation of personal data.

6.3.1 Volume of data: the economies of scale

Economies of scale depends on which kind of data were collected by the firm and on the quality of the analytic tools employed. Scale returns may be low when data are used for inference purpose, but higher for other applications. We can have a clear example of the return to scale importance in the data-driven markets considering the cases of search engines and of Artificial Intelligence (A.I). Both are fundamentally based on trial-and-error experiments (the so called "learning-by-doing" mechanism). In the case of search engine, the more trial-and-error experiments, the more the search engine's algorithms can learn of consumer preferences, the more relevant the search results will be, which in turn will likely attract others to use the search engine. "This positive feedback makes the strong get stronger and the weak get weaker, leading to extreme outcomes".[81] There are, as the competition authorities and OECD found, nonlinear, increasing returns to scale from searches and personal data. The smaller search engine may perform well in terms of quality for popular searches, while struggling instead for the less frequent tail inquiries, where the sample size becomes relevant. For search services, the economies of scale are lower for head queries which are frequently entered by users than for (rarer) tail queries[82].

There is not clear empirical evidence on the extent of these scale economies. There are contrasting opinions in the scholars' debate and the question should be tested a case-by-case. An issue which have significative impact on competition is the claimed necessity of having more data to improve the quality of applications and algorithms. According to the CERRE report this claim should be carefully analysed by agencies[83].

.

[81] OECD (2004), *Data-Driven Innovation for Growth and Well-Being: Interim Synthesis Report*, p. 29, http://www.oecd.org/sti/inno/data-driven-innovation-interim-synthesis.pdf.

[82] As noted by the Monopolkommission (2015, para 202): "While the added value of a frequently searched term can thus be very low, seldom-made search queries may make a major contribution towards improving search results. Such infrequent search queries are likely to particularly include those search queries concerning for instance current events with regard to which there is as yet no information on users' conduct, and search queries consisting of several terms, long-tail queries".

[83] For instance, in the context of the Microsoft/Yahoo! Search Business merger decision, Microsoft argued that with larger scale it is easier to test the algorithm and to experiment more and faster as traffic volume increases, since a smaller proportion of total traffic is involved in the tests. See: Commission Decision of 18 February 2010, Case M. 5727 *Microsoft/Yahoo! Search Business*, par. 162 and 223.

Learning-by-doing characterize not only search algorithms but also artificial intelligence. For example, after its WhatsApp acquisition, Facebook announced a beta version of 'M', its 'digital assistant' able to replace most of the user's web searches with a chat app on Facebook Messenger.[84] Like Apple's Siri, Microsoft's Cortana, and Google's voice-recognition systems, Facebook's technology is based on machine learning. Here, too, the entry barriers may appear low if the data-driven network effects are not considered. M's code and algorithms are largely open source, but here the key asset is the scale of data and the ability of the algorithm to learn by trial-by-error[85]. Previously, to compete against Facebook, an entrant willing to reach the scale necessary to improve its machine-learning could have partnered with WhatsApp. That option is no more available on the market. In addition to this, self-learning analytics tools exhibit steeper experience curves and they may increase the first-mover advantage, making the entry of latecomer competitors more difficult. Their only remaining entry strategies then may be the acquisition of algorithms or investments in their own new tools operating in a different manner[86].

6.3.2 Variety of data: the economies of scope

We have seen in chapter 4, that a characteristic of big data resides in the capacity and the importance of combining different types of data, which brings to economies of scope. The diversification of services leads to even better insights if data linkage is possible. Data linkage enables 'super-additive' insights, leading to increasing 'returns to scope'. The fusion of data from different sources produce a value that is greater than the sum of its isolated parts[87].

The higher the number of people using a company's service, the more data are collected and easier is to create detailed user profiles and to refine algorithms. The company increases its efficiency in targeting users with the most relevant information at critical purchasing moments. A perfect example is Google, which can aggregate and analyse the variety of data collected across its several services (such as learning of a person's plans from an email, a search query, a video watched on YouTube, a website visited via the Chrome, or information in the user's calendar) to add parameters to its algorithm that can better predict more personalized search results.

The European Commission stated in the Google/DoubleClick merger decision that "competition based on the quality of collected data is not only decided by virtue of the sheer size of the respective databases, but also determined by the different types of data the competitors have access to and the question which type eventually will prove to be the most useful for internet advertising purposes."[88] This is also an empirical question which should be tested in each case on the basis of the type of data and application questioned. In particular, the necessity of having more variety of data to improve the quality of the application and the algorithm should be carefully analysed.

---

[84] Mims C., 'Ask M for Help: Facebook Tests New Digital Assistant: Single Interface Could Replace Web Searches and Apps on Mobile Devices', *Wall Street Journal*, 9 November 2015, http://www.wsj.com/articles/ask-m-for-help-facebook-tests-new-digital-assistant-1447045202

[85] Stucke M.E. & Grunes A.P., (2016), *Big Data and Competition Policy*, Oxford University Press, p.181

[86] CERRE report, supra, p. 35

[87] OECD, (2014), *Data-Driven Innovation for Growth and Well-Being: Interim Synthesis Report*, p 29, http://www.oecd.org/sti/inno/data-driven-innovation-interim-synthesis.pdf

[88] Commission Decision of 11 March 2008, Case M.4731 *Google/ DoubleClick*, para. 273

6.3.3 Depreciation value of the data and velocity of the analysis

For many types of data the depreciation rate is very high. Their value is, most of the time, impermanent and relevant only for a short time[89]. For instance, historical data may be comparatively less valuable for some services whose efficient functioning is dependent on the availability of recent and fresh data. Search engines are a typical example. Their algorithms continuously need new data to provide the most relevant results to new searches entered by users.

However, even admitting that the control over these types of data might not give per se a sustainable competitive advantage[90], they may still become important in the moment in which they are capitalised and transformed in more permanent value, used to improve existing applications and to further develop algorithms. It is interesting to notice for the purpose of our discussion that personal data like names, gender, date of birth, address are characterised by a depreciation rate much slower than other categories of data. Therefore, they can potentially bring higher and durable benefits to the data controller.

6.4 Relationships between data collection and analysis: feedback loops

Since the different parts of the big data value chain are closely related, they may be some feedback loops between data collection and data analysis which decrease the cost of the former[91]. We will first look at traditional spill-over effects, and then analyse why personal data amplify the network effects.

As the UK competition authority observed, 'generally, where there is a two-sided platform, there is more value to both sides of having more users'[92]. Relying on the foundational work of economists Jean-Charles Rochet, Jean Tirole, and David Evans on multi-sided markets, the OECD identified indirect spill-over effects as one of the three fundamental aspects of multi-sided platforms: '[...] the value that a customer on one side realizes from the platform increases with the number of customers on the other side. […] A search platform is more valuable to advertisers if it is more likely that it will reach a larger number of potential buyers. It is more valuable to users looking to buy something if there are more advertisers attracted to the platform because that makes it more likely that the user will see a relevant advertisement. It is often the strength of these indirect network effects that determines whether the two-sidedness matters enough to have a substantive effect on the results of economic analysis, or whether it is only an interesting curiosity'.[93]

---

[89] Schepp and Wambach (2016); Sokol and Comerford (2016); UK Competition & Markets Authority (2015, para 3.6)

[90] 'It might not be easy to build a strong market position using data that quickly goes out of date. So, we need to look at the type of data, to see if it stays valuable': Competition Commissioner Vestager, 'Competition in a big data world', DLD 16 Munich, Speech 17 January 2016.

[91] Graef I., (2016), *EU Competition Law, Data Protection and Online Platforms: Data as Essential Facility*, Kluwer Law International; OECD, (2016), *Big data: Bringing competition policy to the digital era*

[92] Office of Fair Trading (OFT), *ME/6167/13: Completed Acquisition by Motorola Mobility Holding (Google, Inc.) of Waze Mobile Limited*, 11 November 2013, para 19 (OFT, *Google/Waze*). http://webarchive.nationalarchives.gov.uk/20140402142426/http:/www.oft.gov.uk/shared_oft/mergers_ea02/2013/motorola.pdf

[93] OECD, *Policy Roundtables: Two-Sided Markets*, December 2009, p. 29.

This is true both for traditional media platforms, like television, radio, and newspapers, and for online platforms, like YouTube, Facebook, and search engines. However, unlike television, radio, and newspaper advertisers, online platforms, because of the many possible use of collect data, are characterised by more dynamic data-driven network effects, as we will see very soon. In particular, personal data amplify these spill-over effects: 'The reuse of data generates huge returns to scale and scope which lead to positive feedback loops in favour of the business on one side of the market, which in turn reinforces success in the other side(s) of the market'.[94]

A first feedback loop, which creates a network effect, is linked to the number of users as depicted in Figure 1 below and runs as follows[95]: (i) more users means more data; (ii) which in turn, means better quality of the service in a general as well as in a personalised way (on the basis of the profile that has been built of a specific user); (iii) which in turn, attracts even more users to the service.

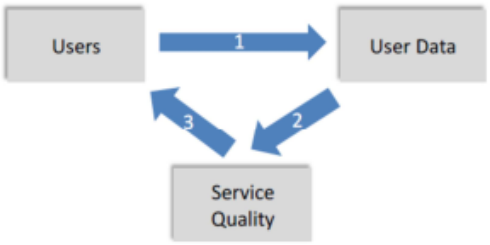


Figure 4: The user feedback loop[96]

In the presence of this feedback loop, new and small platforms have to face higher data collection costs than larger ones[97]. However, the existence and size of this feedback loop is not straightforward, ultimately depending on the magnitude of the correlation between service quality and data processing.

The second feedback loop[98] , as depicted in Figure 5, is mainly based on the monetisation mechanisms of multi-sided platforms. It runs as follows: (i) a bigger users base brings more data; (ii) better targeting is possible; (iii) monetisation increases through pay-per-click models: users are more likely to click on the ads; (iv) the higher attention to ads attracts advertisers; (v) the provider revenues increases; (vi) the provider is able to invest the revenues to improve quality and gain more users; (vii) if the user base increases, the number of advertisers increase too.

http://www.oecd.org/daf/competition/44445730.pdf. The other fundamental elements of two-sided platforms are 'the existence of two distinct groups of customers, who need each other in some way, and who rely on the platform to intermediate transactions between them' and the 'non-neutrality of the price structure', whereby the 'platform can affect the volume of transactions by charging more to one side of the market and reducing the price paid by the other side by an equal amount'. Ibid.

[94] OECD, *Data-Driven Innovation*, supra, p 29.

[95] Autorité de la concurrence and Bundeskartellamt (2016), *Competition law and data*.

[96] De Streel A., Bourreau M., Graef I., (2017), *Big Data and Competition Policy: Market power, personalised pricing and advertising*, CERRE, p.35

[97] Pasquale F.A. (2013), "Privacy, Antitrust and Power", *Georges Mason Law Review* 20(4), 1009-1024; Ezrachi A. and Stucke M.E. (2016), *Virtual Competition: The Promise and Perils of the Algorithm Driven Economy*, Harvard University Press.

[98] As presented by the CERRE report mentioned and cited above

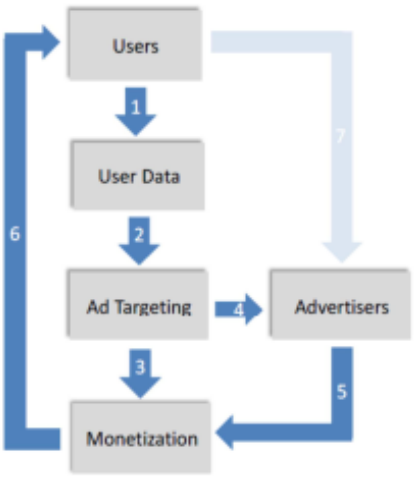


Figure 5: The monetisation feedback loop[99]

When this second feedback loop is in place, the firms who are not able to collect enough data, to target their ads and attract advertisers, have less resource to invest and are less likely to increase the number of their users. The existence and the intensity of this feedback loop needs to be tested on a case-by-case basis and depends on (i) the relationship between the volume of data and the improvement of ad targeting algorithm, (ii) the relationship between the quality of ad targeting and the attraction of advertisers, and (iii) how the platform invests revenues and finances service improvement[100].

Both the feedback loops presented may be amplified by the development of artificial intelligence, which magnifies the relationship between data and service quality in the first loop, and the correlation between data and ads targeting in the second one. Again, this impact needs to be tested only case-by-case and depends crucially on the type of data and on the type of self-learning algorithm. Facebook's social network provides a good example of these feedback loops dynamics.

6.5 Facebook

Facebook's growth in active users on the free side spills over by attracting, on the other side, more advertisers which are interested in reaching these users. Here again data amplify the network effects. First, Facebook does not create many original contents. Mostly all the information attracting new users is due to the free labour of the users already registered. In August 2011, 'Facebook said the average user created 90 pieces of content a month, including news stories and photo albums'.[101] In 2014, users shared 50 billion pieces of content from other apps and websites[102]. Facebook noted how it was '"vital" to encourage a broad range of users to contribute content'[103]. When users slowed down in providing data, Facebook started to nudge them. In the third quarter of 2015, the number of posts was

[99] De Streel A., Bourreau M., Graef I., *Big Data and Competition Policy: Market power, personalised pricing and advertising*, CERRE, 2017, p.36
[100] Ibid., p.37
[101] Seetharaman D., 'Facebook Prods Users to Share a Bit More: Amount of New Content Posted Has Slipped, Leading Social Network to Try to Prompt Conversation', *Wall Street Journal*,2 November 2015, http://www.wsj.com/articles/facebook-prods-users-to-share-a-bit-more-144652072
[102] Ibid.
[103] Ibid.

decreasing: '34% of Facebook users updated their status, and 37% shared their own photos, down from 50% and 59%, respectively, in the same period a year earlier'[104]. So, Facebook began nudging people to post more. Using individuals' likes and location, Facebook stimulated conversations on the social network placing posts related to ongoing events at the top of users' news feeds. Facebook's strategy seemed to work. Second, besides providing the data which convince others to spend time on the social network, users provide themselves the information necessary for advertisers to target them with behavioural ads. As the *New York Times* noted, 'everything you do on Facebook can be used by marketers.'[105] Third, many Facebook users, besides passively providing their personal data, become endorsers when they 'like' a product, advertisement, or company. The more users spend time on Facebook, the more they help the platform to sell ads. Fourth, the overall volume and variety of the personal data help advertisers identify trends and trendsetters. Thus, Facebook benefits from network effects on the demand side and on the supply side, where the volume and variety of data is quickly analysed and used for advertising and for the provision new products and services. All these points clarify why the volume, velocity, variety, and value of personal data accelerate as much as the social network grows.

6.6 Some implications from data-driven network effects

Grunes and Stucke[106] list some relevant features of data-driven network effects. We have already seen the first one: the increasing returns to scale from data can foster a positive feedback loop, depending on the volume, variety and value of the data collected.

Second, the quality of the algorithm may be less important than being able to access a lot of data. An entrant might have a superior algorithm, but only a few platforms like Google's, Apple's, Facebook's, and Amazon's have their scale of users and their data. Having control over huge amount of personal data and being able to quickly analyse them provide a critical competitive advantage. The technology for an app may be off the shelf but data is the key input.

Third, data-driven network effects in online markets can amplify the stakes of an increase and decrease of users. Depending on the network effect, the loss of users can degrade the product's quality and reduce the attractiveness for users, advertisers, or sellers. If a quality gap emerges and becomes evident to consumers, the feedback loop accelerates, attracting both new users and users from rival products.

Fourth, quality under data-driven network effects generally increases with the number of people using the product, but the incremental improvement will slow down as the sample size (N) approaches all. The minimum efficient scale can be quite large in some industries[107] and the scale curve may not be uniform, since data-driven services need robust and representative samples.

---

[104] Ibid

[105] Goel V., 'Flipping the Switches on Facebook's Privacy Controls', *New York Times*,29 January 2014, http://www.nytimes.com/2014/01/30/technology/personaltech/on-facebookdeciding-who-knows-youre-adog.html.

[106] Stucke M.E. & Grunes A.P., (2016), *Big Data and Competition Policy*, Oxford University Press, p.202

[107] The competition agencies, for example, considered that neither Microsoft nor Yahoo! were at the minimum efficient scale at the time of their joint venture. In September 2009, according to comScore, Americans conducted 13.8 billion searches, of which Google sites accounted for 9 billion searches, followed by Yahoo! sites (2.6 billion),

Fifth, the data-driven network effect in some markets will be localized, while in other markets can be leveraged across broader regions. If many New Yorkers use Waze, this does not benefit those stuck in traffic in Los Angeles, but for example, in search engines, the network effects can be broader geographically.

Sixth, there is the potential for the market to '"tip", so that there is one leading player even where le there is still competition.[108] Once the market tips, it is harder for smaller competitors to scale up and displace the dominant company.[109]

Seventh, since data-driven network effects do not necessarily advantage the first mover in every market, the incentives for both anticompetitive and procompetitive behaviour increase. When the stakes are so great, competition can be fierce, but there also strong incentives to adopt anticompetitive practices and merge to tip the market. The feedback loop can reinforce dominance and prevent a rival's platform from increasing. The strong will likely get stronger on both sides of the multi-sided market.[110] Network effects are not necessarily evil: after all, users' welfare and utility generally increase when others join the platform. On the other side, these data-driven effects (traditional, scale of data/trial-by-error, scope of data, and spill-over) provide huge opportunity to dominant online firms to adopt anticompetitive practices and protect their monopoly.

Conclusion

In this chapter we have analysed and explained which are the competitive implications and dynamics involved in data-driven markets. We have showed how relevant entry barriers can be in the digital competition, which traditionally has been considered as a sort of easy space to access from a stream of literature.

To make our reference framework more complete, in anticipation of the last and conclusive section, it is now time to address the issue of privacy. Data protection authorities are very active and important in the digital world, having their jurisdiction on many dimensions of the online experience, not only on those fundamentally economic-related. In order to prepare the final discussion, we will now see how economics has theorized the agents' behaviours in terms of privacy preferences. How agents behave in terms of privacy preferences is an important parameter in assessing consumer welfare and the potential harm for consumers deriving from anticompetitive practices.

Microsoft sites (1.3 billion), Ask Network (541 million), and AOL LLC (416 million). Even if Yahoo! and Microsoft averaged over 80 and 40 million searches per day, respectively, they were still at a disadvantage.

[108] UK Office of Fair Trading (OFT), *ME/6167/13: Completed Acquisition by Motorola Mobility Holding (Google, Inc.) of Waze Mobile Limited*, 17 December 2013, para 44 n 28 ('OFT, Google/Waze'). http://webarchive.nationalarchives.gov.uk/20140402142426/http:/www.oft.gov.uk/shared_oft/mergers_ea02/2013/motorola.pdf.

[109] UK Competition and Markets Authority,(2015), *The Commercial Use of Consumer Data: Report on the CMA's Call for Information*, para 3.51. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/435817/The_commercial_use_of_consumer_data.pdf (receiving 'a number of comments from firms that did not have access to consumers to collect data directly themselves, and commented that a lack of access to data at a particular scale, or of sufficient breadth to equal that of an incumbent was a barrier. […] One respondent noted that the challenges posed by a lack of access to data were magnified by the two-sided nature of the markets and the presence of large established firms.').

[110] OECD, (2014), *Data-Driven Innovation for Growth and Well-being: Interim Synthesis Report*, p. 58

Section II – Economics of Privacy: Literature and Welfare implications

7. Introduction

In this chapter we will move some steps in the field of Economics of Privacy. We are particularly interested in understanding how economic agents behave in terms of privacy preferences, which are the responses to their demand by the market, and which are the dynamics and factors influencing this interaction. We will see further on that the difficult intelligibility of consumers preferences has a particular weight in the two cases analysed in the third section. Users are often unable to navigate the complex trade-offs implied by data protection choices and have to face an online "hostile" environment to privacy policies, full of information asymmetries and purposely designed in a deceptive way. The authorities always have consumer welfare guiding them in the proceedings and in the final decisions. When dealing with privacy, Authorities lack of a clear economic framework of analysis guiding them in the estimation of consumer welfare. As we will see, privacy has most of the characteristics typically attributed to non-price parameters of competition, and even when included in this framework of analysis, it still constitutes a sort of grey area for competition law. In addition to this, as we will explore in the last chapter, the literature on welfare effects of different levels of disclosure/protection of personal information, has provided, so far, only mixed evidence.

8. Definition of Privacy and its features

Privacy is a difficult concept to define. There can be different descriptions of it: as protection of someone's personal space; as control over and safeguard of personal information; as an aspect of dignity, autonomy and human freedom. Ultimately, all these definitions have a common essential feature: they are based on the distinction of boundaries between the self and the others, between private and shared[111]. Economics of privacy, which is the main framework of our analysis, studies the trade-offs associated with the balancing of the public and private sphere of interest between individuals, organizations, and governments. Economists' focus on privacy has been primarily on its *informational* dimension: especially the trade-offs arising from protecting or sharing of *personal data.*

As we have seen in Part I, in today's digital markets, individuals are no longer mere consumers of information, but also public producers of often highly personal data. Individuals' personal information are business assets that can be used to target services or offers, to provide relevant advertising, or to be traded with other parties. The trade-offs between protecting or sharing personal information are difficult for the data subject, for data controllers and for society as a whole[112]. There can be multiple benefits and costs, often amplified by the positive and negative externalities arising from the creation and transmission of data.

[111] Acquisti A., Taylor C. R. and Wagman L., (2016) The Economics of Privacy, *Journal of Economic Literature*, Vol. 52, No. 2, 2016.

[112] This difficult calculus and all the implications related to it are well explained and discussed by Acquisti, Taylor and Wagma cited above.

At the individual level, economic benefits from disclosing personal data may be personalized services, discounts and better tracking on search engines. Conversely, protecting personal information may become an opportunity cost. Externalities may be relevant for individuals, too: a user benefits from others sharing their ranking of movies or restaurants, but he can suffer a cost as well when merchant's analytic tools target him and predict his reservation price. In fact, the individual's cost or ability to protects his personal data is a function of the privacy choices made by others. A high level of personal privacy may be very expensive if everybody behaves differently, or even infeasible (data still may be inferred). This kind of externalities are obviously operative at the society level, too. On one side, the aggregation of online searches may signal phenomena like unknown interactions between pharmaceutical drugs, or even be useful to detect the early spreading of epidemics[113]. On the other side, a diffused comfort with the sharing of data among citizens may bring to a general acceptance of intrusive surveillance programs. Dangers may come from events or fact which are hidden: for instance, insider trading or even some legitimate fringe opinions in the population. Sometimes instead it is beneficial to suppress certain types of information: i.e., concealing of juvenile criminal records as applied in some jurisdictions.

Privacy and personal information reveal some peculiar characteristics once they are analysed as economic goods. Taylor, Wagman and Acquisti listed some of these feautures[114]. First, when shared, personal information can have characteristics of a public good, like non-rivalry and non-excludability[115]: it is often difficult to prevent the access and duplication of released data by other parties, or to have control on its secondary uses.

Second, disclosing data often causes informational asymmetries between data holder and data subject. Therefore, privacy trade-offs are also inherently intertemporal: revealing information often carries an immediate benefit, whereas the costs are often uncertain, and are incurred later in time.

Third, privacy trade-offs often mix the tangible (i.e. a discount), with the intangible (i.e. the psychological discomfort of seeing something very personal exposed without consent), and the nearly incommensurable (the effect on society of surveillance).

Fourth, privacy has elements of both a final good (one valued for its own sake), and an intermediate good.

Fifth, it is not always obvious how to properly value privacy and personal data. This last point is particularly interesting. The value of keeping some personal information protected or not is almost entirely context-dependent and contingent on uncertain combinations of factors. In fact, the value and sensitivity of one piece of personal information matter differently to different people and change overtime (your online activity from five years ago may not be interesting for an advertiser), depending also on the other pieces of data with which can be combined with.

The traditional economic approach to address these questions is that the market reflects the reservation prices of the different agents, capturing accurately the final price of a good. This approach is not fully applicable to personal data. Nowadays, data subjects are not active players in a recognized

[113] See White et al., (2013), Web-scale pharmacovigilance: Listening to signals from the crowd. *Journal of the American Medical Informatics Association*, {2012. and Dugas et al., (2012), Google flu trends: Correlation with emergency department influenza rates and crowding metrics. *Clinical infectious diseases 54* (4), 463{469.
[114] Acquisti, Taylor and Wagman (2016), supra, p.5
[115] Ibid, p.5

and open market for data. Personal information is only traded among firms, but consumers do not have access themselves to this trade, they cannot buy back their data or offer them for sale. Moreover, as we will see in the next chapter, studies on individuals' behaviour and awareness in terms of privacy trade-offs cast many doubts over the market capacity to capture agents' true privacy valuations[116]. By using free apps, social networks and search engines, individual do trade their personal data daily. The point is that for firms data is the essential part of the transaction, whereas it is only a secondary and often intangible aspect for data subjects. Therefore, applying the principle of revealed preferences, we are not inferring appropriately people's valuations for their personal data. In the next section, we will explain further the problem implicit in the adoption of the revealed-preferences argument. Particularly important in this sense is the debate surrounding the so-called "privacy paradox".

9. Consumer Behaviour and the Privacy Paradox

"We communicate using e-mails, texts, and social media; find partners on dating sites; learn via online courses; seek responses to mundane and sensitive questions using search engines; read news and books in the cloud; navigate streets with geo-tracking systems; and celebrate our new-borns, and mourn our dead, on social media profiles. Through these and other activities, we reveal information—knowingly or not—to one another, to commercial entities, and to our governments"[117].

Although privacy concerns seem to vary with context as well as personal traits[118], there are several surveys of US respondents proving that privacy is one of the most significant concerns of Internet users[119]. A 2014 report by the Pew Research Center, found that the majority of US adults (93%) believes that is important to have control of who can collect information about them; but only 9% of them think that they have, in fact, "a lot" of control over their personal data[120]. Likewise, 72 per cent of European Internet users 'still worry that they are being asked for too much personal data online'[121]. Notwithstanding these statements, most consumers remain frequent users of privacy invasive digital services, whose business models is indeed based on tracking and sharing personal information with unknown third parties. This is what scholars have called "Privacy Paradox": the proven and recurrent dichotomy between attitudes, intentions, and actual behaviours in terms of individual privacy preferences.

An insight is that people routinely engage in mental trade-offs of privacy concerns and privacy benefits, or a so-called "privacy calculus"[122]. This context-dependent calculus leads to potentially opposite situations in terms of data protection. Privacy is a modulation of what a person wants to protect and what she wants to share at any given moment and in any given context. Even here, we have some

[116] Berthold, S. and R. Böhme (2010). Valuating privacy with option pricing theory. In *Economics of information security and privacy*, pp. 187. Springer.
[117] Acquisti, A., L. Brandimarte, and G. Loewenstein (2015). Privacy and human behavior in the age of information. *Science 347*(6221), 509{514.
[118] Ibid.
[119] Acquisti, Taylor, Wagman (2016), supra, p.39
[120] Madden M. and Rainie L., (2015), 'Americans' Attitudes About Privacy, Security and Surveillance', *Pew Research Cente*r, http://www.pewinternet.org/fles/2015/05/Privacy-and-Security-Attitudes-5.19.15_FINAL.pdf.
[121] European Commission, (2015) *Why We Need a Digital Single Market*
[122] Dinev, T. and P. Hart (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research 17* (1), 61{80

interesting evidence proving that consumers are not indifferent about their privacy and do not easily trade it for some cheaper or discounted products or services. A 2015 survey of 1,506 American adults found[123]:

- 91 per cent disagreed (77 per cent of them strongly) that 'if companies give me a discount, it is a fair exchange for them to collect information about me without my knowing';
- 71 per cent disagreed (53 per cent of them strongly) that 'it's fair for an online or physical store to monitor what I'm doing online when I'm there, in exchange for letting me use the store's wireless internet, or Wi-Fi, without charge';
- 55 per cent disagreed (38 per cent of them strongly) that 'it's okay if a store where I shop uses information it has about me to create a picture of me that improves the services they provide for me.'

Contrary to the popular assumption that age affects views about privacy, younger consumers in another survey were as concerned about privacy as older ones.[124]Is this dichotomy real or imaginary? Do people actually care about privacy? If they do, how much exactly do they value the protection of their personal data? Empirical evidence of dichotomies between specific attitudes or preferences and actual behaviours have been largely uncovered[125]. Consider, for instance, Turow et al. (2009), who find that 66% of Americans do not wish to receive targeted advertisements while the big majority of them online services, which indeed operate through targeted advertisements.

The questions above may seem trivial, but they are instead very important to solve a theoretical issue related to the welfare of economic agents online. "Revealed preference" arguments, since technologies for information sharing have been more successful than protection technologies, would conclude that individuals hold overall low valuations of privacy. If the consumers were concerned about privacy, they would behave differently. This traditional way of reasoning assumes that the consumers' 'true' privacy preferences are those revealed through their online activity. The point to be remarked, however, is that we can generally infer consumers' privacy preferences from their choices only when consumers are fully informed about their choice's benefits and costs (in this case, privacy risks), and the marketplace offers a competitive array of options that match actual privacy preferences. This is not the case. Several problems exist with this assumption. In this next section we will highlight them.

The assumed consistency of preferences for privacy is complicated by the existence of many, coexisting, and not mutually exclusive different factors. In addition to the primal human instinct for socialization and recognition, which is purely subjective, consumers face various decision-making hurdles dealing with privacy, especially online, such as asymmetric information, bounded rationality, behavioural biases, and various heuristics. Because of these hurdles, it is difficult to pinpoint reliably the valuations that consumers assign to their privacy or to their personal data[126]. Acquisti,

[123] Joseph Turow, Michael Hennessy, and Nora Draper, 'The Trade-off Fallacy: How Marketers Are Misrepresenting American Consumers and Opening Them Up to Exploitation', University of Pennsylvania Annenberg School of Communication, June 2015, p 4

[124] Chris Jay Hoofnagle et al, (2010), 'How Different are Young Adults from Older Adults When it Comes to Information Privacy Attitudes and Policies?'

[125] See Acquisti, A. and R. Gross (2006). Imagined communities: Awareness, information sharing, and privacy on the Facebook. In *Privacy enhancing technologies*, pp. 36{58. Springer; and Turow et al. (2009) Americans reject tailored advertising and three activities that enable it. Working paper.

[126] Acquisti, Taylor and Wagman, (2016), supra, p.41

Brandimarte and Loewenstein[127] individuated three main factors which heavily impact on individuals' privacy behaviours and that can help us to better understand consumers' choices: context-dependence, uncertainty, malleability. We have already mentioned **context-dependence** of privacy choices and behaviours. What we can add is that there many behavioural biases impacting privacy preferences online, apart from the general cultural, motivational and situational differences normally existing. With online interactions, many of common-sense and real-world practices may be distorted. Separating online and offline identities, as well as meeting our and others' expectations regarding privacy becomes more difficult.

Another factor individuated is **malleability** of privacy preferences: various, sometimes subtle, factors can be used to affect privacy concerns. While individuals are often naïve in terms of privacy protection, the entities whose business models is pivoted on data collection are much more sophisticated. They have all the incentives in taking advantage of behavioural and psychological biases to promote disclosure and profit.[128] Here some examples. Default settings are an important tool used by different entities to affect information disclosure. Consumers' behaviour may reflect the privacy default rather than their privacy preference.[129] In addition, firms can manipulate consumers' behaviour by giving them the illusion of control. The firm might offer the option of deleting tracking cookies or personal information on their servers, knowing that most users will likely forget to do so regularly. They might exploit data protection tools, originally intended to protect consumers, in order to create "fake" protected online environments. For instance, 62% of respondents to a survey believed thought that the mere existence of a privacy policy precludes a website to share personal information without permission[130]. Research has highlighted not only that the majority of Internet users do not read privacy policies, but also that few users would benefit from doing so; since nearly half of a sample of online privacy policies was written in language not comprehensible for most Internet users[131]. Finally, websites may use design features to nudge users into disclosing data, a practice referred to as "malicious interface design"[132]. An important strategy is also not to "ring alarm bells" when it comes to data collection, in order to prevent users to engage in "negative reactance"[133].

The last determinant factor affecting privacy preferences individuated by Acquisti, Brandimarte and Loewenstein is **uncertainty**, mostly deriving from the strong asymmetric information typical of online eco-systems. Lacking information about data controllers' practices, users are likely to be uncertain about how much to share. The situation is exacerbated by the fact that privacy harms can be sometimes intangible and often not immediate. In one study, individuals were asked to use a search

[127] Acquisti, A., L. Brandimarte, and G. Loewenstein (2015), supra

[128] Calo R., (2014), Digital Market Manipulation, *82 George Washington Law Review* 995; University of Washington School of Law Research Paper No. 2013-27.

[129] Johnson E., Bellman S. & Lohse, G. (2002). Defaults, Framing and Privacy: Why Opting In-Opting Out1. *Marketing Letters*. 13. 5-15.

[130] C.J. Hoofnagle, J. Urban, (2014), Alan Westin's Privacy Homo Economicus, 49 *Wake Forest Law Review* 261 (2014); UC Berkeley Public Law Research Paper No. 2434800

[131] Jensen C., Potts C. & Jensen C., (2005). Privacy practices of Internet users: Self-reports versus observed behavior. *International Journal of Human-Computer Studies*. 63. 203-227.

[132] G. Conti, E. Sobiesk, Malicious Interface Design: Exploiting the User (19th International Conference on World Wide Web, ACM, Raleigh, 2010), pp. 271–280

[133] White, Tiffany Barnett, et al. "Getting Too Personal: Reactance to Highly Personalized Email Solicitations." *Marketing Letters*, vol. 19, no. 1, 2008, pp. 39–50.

engine to purchase batteries and sex toys.[134] When the search engine provided only the merchants' websites and a comparison of prices, most people did not pay attention to the manufacturers' privacy policies and chose the lowest price. But when salient and easily accessible information about the differences in privacy policies were provided, most people opted for merchants charging a 5 percent higher price while offering greater privacy protection.

The second source of privacy uncertainty relates to the nature of preferences themselves[135]: even when aware of the consequences of privacy decisions, individuals cannot quantify how much they like goods, services, or other people. Privacy does not seem to be an exception. Preference uncertainty is evident not only in studies comparing stated attitudes with behaviours, but also in those estimating monetary valuations of privacy. Several studies attempted to quantify the value of data for both organizations and for end-users. For instance, Olejnik et al. (2014) found pieces of users' browsing histories traded in the online advertising market for less than $0.0005 per person. Hann et al. (2007) quantified the value assigned to the protection of their data by US citizens to an amount between $30.49 and $44.62. Similarly, Savage and Waldman (2013) find that consumers are willing to make a one-time payment of $2.28 to hide their browser history, $4.05 for their contacts list, $1.19 for their location, $1.75 for their phone's identification number, $3.58 for the contents of their text messages, and $2.12 to eliminate advertising[136]. It is important to notice however that, in general, the conclusions of all these kinds of studies are seriously affected by even small changes in contexts and scenarios, in the price and in product considered: a premium price of roughly one dollar for better privacy policy may be accepted for a 15$ dollar good but, in other situations, consumer may prefer to purchase goods like a cinema ticket or a DVD from a more privacy-invasive merchant, than from a costlier (1 Euro more) but less invasive merchant[137].

These three summarizing factors listed above, and the evidence reported since now well clarify why the "revealed-preferences" theorem cannot really be taken as logically coherent. Even if all the above-mentioned problems were resolved - i.e., consumers know what data are collected and for what purpose; are not influenced by biases and heuristics; and have enough knowledge to make informed cost–benefit choices —a last problem with the theorem would be that consumers don't really have the opportunity to choose among a competitive range of options matching their actual privacy preferences. In the next section, we try to further investigate this last complexity.

10. Why market forces did not guarantee more privacy for consumers

The rise of data-driven mergers and business strategies raise several competition policy issues that the authorities must address. In this chapter, we address specifically one of these issues: why market forces are not promoting services affording great privacy protections.

[134] Tsai, J. Y., et al. "The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study." *Information Systems Research*, vol. 22, no. 2, 2011, pp. 254–268.
[135] Slovic, Paul. (1995). The Construction of Preference. American Psychologist. 50. 364-371.
[136] See Olejnik et al., (2014), Selling off privacy at auction. In *ISOC Network and Distributed System Security Symposium*; Hann, I.-H., K.-L. Hui, S.-Y. T. Lee, and I. P. Png (2007). Overcoming online information privacy concerns: An information-processing theory approach. *Journal of Management Information Systems 24*(2), 13{42; Savage, S. and D. Waldman (2013). The value of online privacy. Working Paper
[137] See Tsai et al. (2011); Jentzsch et al. (2012); Preibusch et al. (2013)

One explanation which has been proposed is that consumers—especially younger ones—are not concerned about privacy. But the many surveys we presented clearly undercut this claim. We have already seen in chapter 8 that consumers, when interviewed, prove to be concerned about their privacy. A second possible explanation is that competition, at times, can worsen, rather than improve, the privacy protections. However, this does not rule out the fact that competitive market forces should generally be responsive to consumers' demand for better privacy protections. The fundamental problem in these markets is that consumers lack viable alternatives. This seems to be the most reasonable explanation. The reason why market forces have not offered the privacy protections that individuals demand is the absence of meaningful competition[138].

Normally, we expect competition to pressure firms to deliver the benefits from data-driven strategies, while protecting consumers from the harms associated with monopolization and restraints of trade.[139] If some companies are less transparent over their data policies, then consumers should be able to opt for competitors closely aligned with their privacy preferences. Competition should bring new firms to offer users better services, and provide privacy-enhancing technologies matching their preferences. That is not happening today. As the European Data Protection Supervisor observed, "despite the risks to the personal data of individuals using these services, the market for privacy-enhancing services remains comparatively weak"[140]. The problem is that consumers are often unaware of the which data are collected about them and how they are used. They normally do not interact with data brokers and do not know how their consumer profiles are being used[141], nor do they know who is tracking them across the web and for which purposes.

Data-driven companies don't have any reason to change the state of the art. Unlike consumers, they are not interested in technologies promoting privacy and block ads. Indeed, privacy technologies and legislation represent a threat. They warn investors how additional privacy safeguards and ad blocking technologies would harm their business. For example, in its 2014 Annual Report, Google identifies various risks that could adversely affect its business, financial condition, results of operations, cash flows, and the trading price of its common and capital stock[142]. One risk is that "new technologies could block online ads, which would harm the business."[143] Facebook is also very aware of the threat of privacy innovations to its business model. Like Google, practically all of Facebook's revenue is generated from advertising[144].

---

[138] Stucke M. E and Grunes A. P., (2016), *Big data and competition policy,* Oxford University Press

[139] European Commission, *Guidelines on the Assessment of Non-Horizontal Mergers under the Council Regulation on the Control of Concentrations Between Undertakings*, 18 October 2008, para 10

[140] European Data Protection Supervisor (EDPS), 'Privacy and Competitiveness in the Age of Big Data: The Interplay Between Data Protection, Competition Law and Consumer Protection in the Digital Economy', Preliminary Opinion, March 2014, p. 8 ('EDPS Preliminary Opinion').
https://edps.europa.eu/sites/edp/files/publication/14-03-26_competitition_law_big_data_en.pdf

[141] FTC, *Data Brokers: A Call for Transparency and Accountability*, May 2014, p. iv.
https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf

[142] Google Inc, Annual Report Pursuant to Section 13 or 15(D) of the Securities Exchange Act of 1934 for the fiscal year ended December 31, 2014, p. 12.

[143] Ibid.

[144] Facebook reported advertising revenue at $16.6 billion for the final quarter of 2018, up 30 percent year-over-year. Facebook did not break out advertising revenue by ad product type, but did report 93 percent of ad revenue during the fourth quarter came from mobile advertising.

10.1. Why privacy concerns are not getting answered by the market?

The online markets provided many products and services free of charge, but often at a heavy cost to consumers' privacy. So why hasn't the market responded to their privacy concerns?

One of the possible explanations we listed so far is that competition, at times, makes worse, rather than improve, the situation.[145] Competition becomes a race to the bottom, wherever companies profit by making their privacy policies less transparent.[146] Behavioural economics literature described how in certain cases entry can increase, rather than reduce, behavioural exploitation.[147] Notwithstanding this, markets should still be responsive to consumers' demand for better privacy protections, but are not. The fundamental problem is the lack of viable alternatives.

Here we see the core concern of competition policy—namely the accumulation of market power—intersect with privacy concerns. The reason why market forces don't provide enough privacy protections is the absence of fierce competition. In a 2010 interview, Google's Executive Chairman admitted that the company collected data to be able to deliver better-targeted ads. Eric Schmidt stated that competition prevented Google from abusing people's privacy: 'All of our testing indicates that the vast majority of people are perfectly happy with our policy. And this message is the message that nobody wants to hear so let me say it again: the reality is we make decisions based on what the average user tells us and we do check. And the reason that you should trust us is that if we were to violate that trust people would move immediately to someone else. We're very non-sticky so we have a very high interest in maintaining the trust of those users[148]'.

Schmidt's argument sounds convincing. Google, after all, does not charge people for using its search engine, email, browser, and other products. The problem is that Google violated its privacy policy and different jurisdictions' privacy laws multiple times in the last decade without losing its dominance[149]. The violations have been sanctioned both in the US and in EU, sometimes the subsequent failure to implement the authorities' requirements brought additional fines. They range from the infringement of privacy policies[150], data protection rules[151] (GDPR) and the use of deceptive tactics, to more

https://martechtoday.com/despite-ongoing-criticism-facebook-generates-16-6-billion-in-ad-revenue-during-q4-up-30-yoy-230261

[145] Stucke M. E., 'Is Competition Always Good?', 1 *Journal of Antitrust Enforcement* (2013): p 162.

[146] EDPS Preliminary Opinion, supra, p 11 (noting that, as of 2014, 'relatively few companies in the digital economy have detected financial advantage in enhancing the privacy of their offerings').

[147] Stucke M.E., 'Behavioral Exploitation and its Implications on Competition and Consumer Protection Policies', in Swedish Competition Authority (ed), *The Pros and Cons of Consumer Protection* (Stockholm: Konkurrensverket Swedish Competition Authority 2012), pp 77–122.

[148] Shane Richmond, 'Google's Eric Schmidt: You can Trust Us with Your Data', *The Telegraph*,1 July 2010

[149] For a completer and more detailed list, see: Stucke M. E and Grunes A. P., (2016), *Big data and competition policy,* Oxford University Press, p.62

[150] FTC, 'Google Will Pay $22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser', Press Release, 9 August 2012

[151] Letter from the Article 29 Data Protection Working Party to Larry Page, 16 October 2012, http://www.cnil.fr/fleadmin/documents/en/20121016-letter_google-article_29-FINAL.pdf. See also: CNIL, 'The CNIL's Sanctions Committee Issues a 150 000 € Monetary Penalty to Google Inc', 8 January 2014; FTC, 'FTC Charges Deceptive Privacy Practices in Google's Rollout of Its Buzz Social Network: Google Agrees to Implement Comprehensive Privacy Program to Protect Consumer Data', Press Release, 30 March 2011

clamorous conducts like illegal collection of data through the Google's Street Views cars[152] and billing users millions of dollars through in-app charges incurred by children[153]. Moreover, there were other cases where Google reportedly collected personal data without the person's knowledge.[154]

So, if Google has committed so many major violations, why hasn't it significantly lost its market power? Why haven't the consumers switched to other providers? Either the consumers are not disturbed by these behaviours or they do not have viable alternatives. The former is less likely. A 2014 survey of over 2,500 Americans found that they were more concerned about a company like Google gaining access to their personal data, than the US National Security Agency or their boss, parents, or spouse.[155] An earlier pre-Edward Snowden 2012 survey found that Google was the overwhelming choice among more than half of American adults using a search engine, and that while satisfied with the search results, most users disapproved of their personal information being collected for search results or for targeted advertising.[156]

In a 2015 report, the UK competition authority concluded that 'the balance of power over the collection and use of data had moved from consumers towards businesses'[157]: big data collectors gather information consumers are not aware of, use them without receiving consent, and don't allow to opt-out. It is also noted that, as a result of increasing digitisation, there has been a shift from a primary focus on volunteered information to 'passive' data collection[158].

Data-driven industries, including those offering free services, may be characterised by market power and monopolistic structure. Thus, one fundamental concern is that while governments promote the use of Big Data, they also need to protect citizens from market dominant companies such as Google, Amazon, and Facebook—as well as lesser-known "data-brokers", such as Acxiom and Experian.

To resume, the explanation for market forces not providing the privacy protections that individuals desire is competition-related. Key industries are dominated by a few data-driven companies with low interest in protecting personal privacy while facing little competitive pressure. They can violate rules and laws over privacy, without incurring in serious retaliation from consumers. The result is that data-driven firms in some markets have enough economic power to act to a considerable extent independently of their customers' preferences. Mainstream economics would suggest that if firms were not supplying the level of privacy consumers wanted, there would be new entry or repositioning by competitors attracted by the chance to profit. But, as economist Joseph Farrell has pointed out, if

---

[152] Casey Newton, 'Google Reaches $7 Million Settlement with States over Street View Case', *CNET*, 12 March 2013,

[153] FTC, 'FTC Approves Final Order in Case About Google Billing for Kids' In-App Charges Without Parental Consent', Press Release, 5 December 2014

[154] Public Citizen, *Mission Creep-y: Google Is Quietly Becoming One of the Nation's Most Powerful Political Forces While Expanding Its Information-Collection Empire*, November 2014, p. 35, https://www.citizen.org/documents/Google-Political-Spending-Mission-Creepy.pdf.

[155] Troy M., 'What's Worse than Your Mom Seeing Your Web History? The NSA, Google, *Survata Blog*, 27 October 2014, https://blog.survata.com/whats-worse-than-your-mom-seeing-your-web-history-the-nsa-google

[156] Purcell K., Brenner J., and Rainie L., *Search Engine Use 2012*, Pew Research Center, 9 March 2012, http://www.pewinternet.org/2012/03/09/search-engine-use-2012

[157] UK Competition and Markets Authority, *The Commercial Use of Consumer Data: Report on the CMA's Call for Information*, June 2015, paras 20–1, 4.1–4.42 ('CMA Report')

[158] Ibid.
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/435817/The_commercial_use_of_consumer_data.pdf

consumers have resigned themselves to this situation, an entrant or a competitor would be unable to benefit from privacy-protective promises. The result can be like a self-fulfilling prophecy. Existing companies have little incentive to offer more protection, because it is costly, and new competitors trying to compete on privacy protection will not have that demand that would occur in a well-functioning market. The final outcome is a 'dysfunctional equilibrium.'[159] It is unquestionable that market forces, if left uncontrolled, do not always foster competition; instead, they may bring mergers, consolidation, and concentration, especially in winner-take-all markets. Dominant firms can abuse their power and, they can undertake anticompetitive data-driven strategies to attain or maintain their monopoly.

11. Economics of Privacy: a literature review

We have seen that information asymmetries and heuristics studied by behavioural decision researchers, cast doubts about individual's ability, as rational agents, to optimally navigate privacy trade-offs. These observations bring us to even more questions: are the privacy equilibria benefitting both data holders and data subjects? What is the reallocation of surplus deriving from personal data between the different stakeholders? This surplus should be allocated by market forces (considering privacy as an economic good) or by regulation (treating privacy as a fundamental right)? Which of the agents involved should be favoured by the allocation: the owners of the data or the holders who invested in the collection and processing? These are crucial questions in the moment in which an antitrust authority has to take a decision, but unfortunately, they don't have a clear-cut answer, yet.

Here, for reasons of length and coherence of the text, we can't dive in the wide economic literature of Economics of Privacy. A very extensive and greatly exposed review has been offered by Acquisti, Taylor and Wagman[160]. They present three main historical waves of research: an early wave dating back to the 1970s and early 80s; a middle one active in the 1990s; and a more recent and growing third wave. They also sub-divide the studies according to different online practices, which are more and more getting the attention of the scholars. To sum up the literature and grasp the main insight needed for the purposes of our discussion, it is important to evidence three main themes emerging from the survey[161]: (i) the definition of a single unifying economic theory of privacy is still hard. Privacy issues of economic relevance are involved in different economic contexts. However, it is still possible to have some solid evidence, once we have a delimited framework. (ii) Privacy protection can increase or decrease individual and societal welfare depending on the contexts and specific scenarios. This is largely exposed both by theory and empirical analysis. It is not available an unambiguous and absolute conclusion on its effect in economic terms. (iii) Market interactions often take place without individuals being fully informed about the consequences of their actions.

[159] Joseph Farrell, 'Can Privacy Be Just Another Good?', 10 *J on Telecomm & High Tech L*(2012): pp 258–9

[160] Acquisti, A., Taylor C. R. and Wagman L., (2016), *The Economics of Privacy,* Journal of Economic Literature, Vol. 52, No. 2, 2016; Sloan Foundation Economics Research Paper No. 2580411..

[161] Ibid.

Conclusion

In the last years, economists have gone further in studying many new dimensions opened by the fast-developing digital markets, as data intermediaries, online marketing techniques, price and behavioural discrimination. A whole new stream of literature is blooming around the advent of the Internet of Things technologies, which promise to bring personalisation and behavioural discrimination to unprecedent levels. As said above, it was not possible for us to treat all these subjects. However, we are still facing a lack of a strong and definitive evidence on the welfare implications of all these economic dynamics. Benefits and costs are extremely context-dependent, both for data subjects and data controllers. Therefore, there is not a clear and solid economic framework capable of guiding antitrust authorities in assessing welfare effects on users and firms whenever privacy issues are involved.

Both the theoretical and the empirical studies suggest that the path towards optimally balancing privacy protection and benefits from disclosure is, at the very least, uncertain. Yet, we have some clear points that deserve to be remarked once again: "(i) different stakeholders, including businesses, consumers, and governments, each have different, multi-layered, and often conflicting objectives; (ii) information technologies, privacy concerns, and the economics of privacy evolve constantly, with no single study or policy intervention being able to fully account for future (and even some present) concerns; and (iii) rather than a uniform piece of regulation to address contemporary privacy issues, a nuanced approach - dynamic and individualized to specific markets, contexts, and scenarios - may be necessary"[162].

Section III - The Intersection between Competition Law and Data protection

In this third and last section we will finally see how the concepts illustrated until now become crucial and relevant in the assessment of an antitrust case. We will try to fill a gap, namely the need for in-depth economic analysis of why personal data issues are antitrust issues and should be solved not only by consumer protection and privacy laws but also by competition law.

In particular, we will analyse two different case studies, both involving Facebook: the EC clearing in 2004 of the Facebook/WhatsApp merger and the very debated Bundeskartellamt decision of February 2019. The two cases show two different ways in which competition law and privacy protection intersect.

The Facebook/WhatsApp merger has been considered for many years as a "vanguard case", because of the methodology and the parameters adopted by the Commission. However, this consideration was recently called into question. In the next chapter we will see why, and we will try to understand the limitations and errors of the investigation that could have been addressed through a better consideration of privacy issues. We will able to remark some of the points that we started to define in chapter 6: the collection and analysis of huge amount of data have relevant competitive implications. Privacy was a crucial element in the case and the commission failed to consider fully its competitive

[162] Ibid, p.41

relevance. In the second part we will discuss the Bundeskartellamt decision dated February 2019, which appears to be the new frontier in terms of antitrust investigation in the field of personal data. The German Antitrust Authority has found Facebook exploiting its market power by imposing unfair terms and conditions to users. This decision is very debated at the moment: it is, in fact, the first time that a competition law authority defines an abuse of dominance in the field typically under the jurisdiction of data protection authorities. The case was welcomed with enthusiasm by the incumbent European Data Protection Supervisor Giovanni Buttarelli, but nonetheless, is a thorny decision which may imply unprecedent consequences.

12. The Intersection

One difficult and pressing issue for Competition authorities is to appreciate when privacy concerns are within the scope of competition law. More specifically, the concern is over the acquisition and use of personal data to obtain significant market power. The intersection between privacy and antitrust matters is not always straight-forward. Data-driven strategies may raise privacy concerns but not antitrust ones, and vice versa. Even when this intersection is recognized, it is then delicate to balance the data protection and antitrust interests. Which one of the two will increase consumer welfare? A lessening in data protection might be counterbalanced by better competition/quality?

To explore where privacy and competition intersect, we shall start with the consensus about privacy as a parameter of non-price quality competition. This is a well-accepted and common concept among antitrust authorities and the actual main approach used to deal with privacy in competition law. As several European Commission officials noted, if a website, post-merger, 'would start requiring more personal data from users or supplying such data to third parties as a condition for delivering its "free" product' then this 'could be seen as either increasing its price or as degrading the quality of its product' and infringe competition law.[163] Here, we can already see, beside the quality parameter, another possible approach, which we will develop further later in the text.

US and European competition agencies appear to be open to analyse the loss of privacy as a potential anticompetitive effect in data-driven mergers but still face several challenges. These are the challenges normally related to any other non-price parameter: subjectivity and multi-dimensionality of preferences among consumers, difficulties in defining a standard framework and measures, problems to translate insights in operative and quantitative tools. In addition to these "new" challenges, there are the ones naturally implied by the structure of multi-sided advertising-supported platforms, mainly related to the balancing of benefits and the network effects between the different sides of the platforms: the paying side and the free one.

Finally, competition authorities have generally embraced a methodology of assessment which is prevalently price-centric. Those factors that are easier to measure (such as the merger's likely short-term impact on price, output, or productive efficiency) has become disproportionately important through time. The competition agencies generally acknowledge the importance of parameters of competition even when they can't quantify precisely how they are going to be affected by a merger; but they generally do not challenge a merger for lessening competition primarily on this parameter.

[163] Eleonora Ocello, Cristina Sjödin, and Anatoly Subočs, 'What's Up with Merger Control in the Digital Sector? Lessons from the Facebook/WhatsApp EU Merger Case', 1 *Competition Merger Brief* (February 2015): p 6.

We see this dynamic with quality competition. Rarely competition authorities assess a merger's impact primarily or solely on quality.

12.1 Promoting consumers' privacy interests is a part of quality competition

Non-price parameters are fundamental aspects of competition. Quality drives innovation and economic growth, and decreasing can be as harmful to consumers as a price increase.[164] Thus, maintaining and improving quality are important competition policy concerns. Quality is a broad concept that encompasses also privacy protection.[165] Even though privacy harms can be subjective, so are other quality degradations.

Data-driven mergers in multi-sided markets may substantially lessen competition at different levels, and along certain parameters but not others. Competition may take place in several areas: first, on non-price parameters on the 'free' side of the market; second, on the 'paid' side of the multi-sided market; and third, among firms to collect valuable data as a key input. When the product is free, quality, the European Commission found, will often be a significant parameter of competition.[166]

The problem is that when the product's price is zero and the most important parameter of competition is subjective, multi-dimensional, and difficult to quantify, competition agencies do not have updated tools for market definition, entry barriers assessment, and for the prediction of competitive effects under a unilateral or coordinated effects theory. The 2010 Horizontal Merger Guidelines did not provide an analytical framework to deal with these non-price parameters, such as innovation or quality. Rather than use a SSNIP test (which has been proven not to be appropriate in zero price markets), one possible solution is to inquire about a small, but significant, non-transitory decline in quality (SSNDQ). However, absent well-accepted quantifiable measures of quality (i.e., those available in some industries like health care), the SSNDQ test has been to date unworkable. It is not reliable: apart from the difficulty to find some standard and quantifiable measures of privacy, it is based on the (proven wrong) assumptions that consumers readily detect privacy degradation and are easily able to switch to other better equipped rivals. Because of the information asymmetries, behavioural biases (presented in chapter 9, page 34) and network effects (treated in chapter 6) these assumptions are often not realistic.

12.2 The Facebook/WhatsApp merger

Texting and social networks are huge. Nowadays, WhatsApp is the most used messaging app worldwide, counting 1.6 billion of users, closely followed by Facebook's Messenger with 1.3 billion, and then by the Chinese app WeChat with 1.1 billion users. There are only 25 countries in the world where WhatsApp is not the market leader. WhatsApp and Facebook Messenger are growing about twice as fast as the original Facebook platform (+30% YoY). Currently, WhatsApp has the highest

[164] OECD,(2013), *The Role and Measurement of Quality in Competition Analysis*, p5 (executive summary)
[165] EDPS, (2014), *Privacy and Competitiveness in the Age of Big Data: The Interplay Between Data Protection, Competition Law, and Consumer Protection in the Digital Economy*, Preliminary Opinion, p 17
[166] *Microsoft/Yahoo! Search Business* (Case Comp/M.5727), Commission Decision C(2010) 1077 [2010] OJ C 020/08, para 101; *Microsoft/Skype* (Case Comp/M.6281), Commission Decision C(2011)7279, 7 October 2011, para 81

distribution of all messaging apps worldwide. If you combine all the existing apps belonging to the Facebook Universe, there are only 10 countries in the world where the messenger market leader is not Facebook owned[167].

Both Facebook and many texting apps are free and the currency in these markets is normally users' personal data. Not surprisingly both privacy and Big Data issues arose in 2014 when Facebook announced its largest acquisition to that time, buying WhatsApp for USD 19 billion in cash and stock. Both Facebook and WhatsApp offered popular texting applications for smartphones, already in 2014. Facebook runs his own texting app 'Facebook Messenger' and acquired the photo and video-sharing platform 'Instagram' in 2012. In 2014, 300 million of Facebook's 1.3 billion social network users worldwide were using the Facebook Messenger app.[168]

It was immediately evident that privacy was a relevant parameter of competition: WhatsApp did not sell advertising space or collect a lot of personal data on its mobile app users. It charged users a nominal fee, and promised not to collect names, emails, addresses or other contact information from its users' mobile address book or contact lists other than mobile phone numbers. In contrast, Facebook's texting apps are free, but they are based on the harvests of users' data and targeted advertisement. In addition to this, Facebook messaging was already notorious at the time for its extensive data collection practices.[169] Pre-merger consumers were able to choose between two popular texting apps with different price/privacy trade-offs, the choice was significantly reduced by the proposed acquisition. However, neither the FTC nor European Commission, challenged the merger. Unlike the European Commission, the FTC never publicly commented on the merger's antitrust implications. The Director of the FTC's Bureau of Consumer Protection only warned Facebook about using WhatsApp data in a letter to the parties. She made clear that WhatsApp should have continued to honour its premises to consumers.[170] If Facebook, post-merger, wanted to use data collected by WhatsApp differently from these promises, then it needed the individuals' affirmative consent.

What is interesting in this case is that competition occurred on several levels: on one level, companies competed to attract consumers to spend time on their platforms and their personal data; on a second level, companies competed over the means to collect the personal data (texting apps). On a third level, they competed on the 'paid' advertising side of the multi-sided platform. Thus, the merger could potentially harm several different groups: advertisers, with higher rates; users of text apps (with less quality, innovation, and privacy protection for their data); and lastly competitors who are foreclosed from achieving scale.

---

[167] All these figures are taken from last Global Digital Report published by We Are Social and Hootsuite. Available at: https://wearesocial.com/global-digital-report-2019

[168] European Commission, 'Mergers: Commission Approves Acquisition of WhatsApp by Facebook', Press Release, 3 October 2014

[169] Consumer groups have criticized Facebook's privacy policy: "Facebook messaging is notorious for its extensive data collection practices. When Facebook revamped its messaging system in November 2010, it automatically opted in all Facebook users and initially disabled users' ability to delete individual messages. Without user consent, the new messaging system also pulled data from Facebook's social graph to prioritize messages from certain users. Currently, even when users delete a message, it continues to be stored on Facebook's servers." Electronic Privacy Information Center, In Re WhatsApp, https://epic.org/privacy/internet/ftc/WhatsApp/

[170] Letter from Jessica Rich, Director, Bureau of Consumer Protection to Erin Egan, Chief Privacy Officer, Facebook, Inc and Anne Hoge, General Counsel, WhatsApp Inc, 10 April 2014 ('Rich Letter')

12.3 The European Commission investigation - Case No COMP/M.7217, REGULATION (EC) No 139/2004[171]

Unlike the FTC, the European Commission engaged in a long and extensive investigation before clearing the merger. To its credit, it considered this data-driven merger's impact on both sides of the platform and even the accumulation of user data as a theory of competitive harm. In its proceeding, the European Commission first identified how Facebook offered its social networking platform and texting services for free, in order to collect significant volume of personal data[172], while instead WhatsApp did not amass data on its users for advertising purposes. There was the potential risk of a change in the WhatsApp business model post-merger. That's why, two different theories of harm were considered, both potentially strengthening Facebook position in online advertising by:

(i) introducing advertising on WhatsApp, and/or

(ii) using WhatsApp as a potential source of users' data for the purpose of improving the targeting of Facebook's advertising activities outside WhatsApp.

Under the first theory of harm, Facebook could have reinforced its position in the online-advertising market, introducing targeted ads on WhatsApp by analysing users' data collected from both the messaging apps. The public version of the Commission's decision does not include commercially sensitive information, so we do not have all the facts upon which the Commission relied. It appears from what was published that Facebook could introduce ads on WhatsApp, but it lacked the incentive, because of considerable technical hurdles[173] and the necessary change in WhatsApp privacy policies (likely to upset users and push them to switch). The Commission's analysis, however, did not stop here. Going one step further, it engaged in an 'even if analysis': even if Facebook did introduce ads on the formerly ad-free WhatsApp, it was found that there would 'continue to be a sufficient number of other actual and potential competitors equally well placed as Facebook to offer targeted advertising'.[174]

The Commission's second theory of harm inquired whether Facebook would have used WhatsApp users' data to better target them on Facebook's platform. Facebook reported to have 'no current plans to modify WhatsApp's collection and use of user data'.[175] The Commission never predicted whether or not Facebook would have collected data from WhatsApp users. Even in that hypothetical scenario, the Commission stated that transaction 'would only raise competition concerns if the concentration of data within Facebook's control were such as to strengthen its position in advertising'[176]. According to the Commission that it wasn't the case as there were 'a significant number of market participants that collect data alongside Facebook', namely Google, and 'companies such as Apple, Amazon, eBay,

[171] http://ec.europa.eu/competition/mergers/cases/decisions/m7217_20141003_20310_3962132_EN.pdf
[172] "Facebook collects data regarding the users of its social networking platforms and analyses them in order to serve advertisements on behalf of advertisers, which are "targeted" at each particular user of its social networking platforms." From European Commission, 'Mergers: Commission Approves Acquisition of WhatsApp by Facebook', Press Release, 3 October 2014
[173] European Commission, Case COMP/M.7217 Facebook/WhatsApp, REGULATION (EC) No 139/2004, para 185
[174] Ibid para 179
[175] Ibid para 182
[176] Ibid, para 187

Microsoft, AOL, Yahoo!, Twitter, IAC, LinkedIn, Adobe and Yelp, among others'[177]. The Commission estimated the shares of data collection across the web[178]:

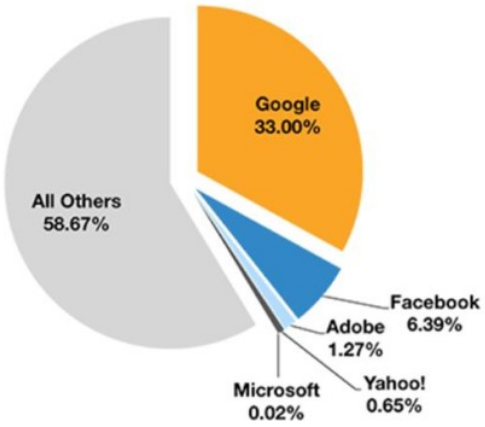


Figure 5: Shares of data collection across the Web[179]

Even under the realization of this second theory of harm, there would have continued to be a large amount of Internet users data valuable for advertising purposes and not within Facebook's exclusive control.[180] On the consumer side, the Commission concluded that the merger was unlikely to lessen competition for texting apps. The Commission indeed recognized that one important, non-price parameter of competition was 'privacy and security, the importance of which varies from user to user, but which are becoming increasingly valued, as shown by the introduction of consumer communications apps specifically addressing privacy and security issues'.[181] The Commission cited the differences in Facebook's and WhatsApp's privacy protections as evidence of their not being close competitors[182]. The consumers would have continued to have a wide choice of alternative communication apps after the transaction, no significant costs preventing switching behaviour were found and network effects were considered unlikely to shield the merged entity from new and existing rivals.[183]

12.4 An evaluation of the EC decision

This decision, at the time, was considered the vanguard of the analysis of data-driven mergers in multi-sided markets, where the product or service is free. Nonetheless, the analysis has some limitations[184].

First, the Commission estimation of overall data market in order to assess the merging companies' market share is not correct. Not all kind of data are fungible or valuable at the same way for the different online services. Data has not intrinsic value, which is indeed use-dependent. For example, data from Microsoft, or Adobe would not have the same value as WhatsApp' data for Facebook.

[177] Ibid para 188
[178] *Source*: ibid
[179] European Commission, Case COMP/M.7217 Facebook/WhatsApp, REGULATION (EC) No 139/2004, para 185
[180] Ibid, para 189
[181] Ibid para 87
[182] Ibid para 102,107
[183] Ibid para 135
[184]Stucke M.E. & Grunes A.P., (2016), *Big Data and Competition Policy*, Oxford University Press,p.79

Second, the remaining amount of data available to other competitors and not exclusive to Facebook may not necessarily provide them the same competitive advantage (and perhaps market power) enjoyed by the merged entity. If other companies could acquire the same type of user data, they may be unable to access, analyse, and capitalize on the data as quickly as Facebook could. Here, velocity and variety can be key factors to consider.

Third, the Commission did not consider the potential combined dataset to be a unique, non-replicable advantage, because of the presence of other services like data brokers. "Competition authorities need to consider not only how much data the merged entity has relative to the outside world, but how much it has relative to what is readily available elsewhere. If only a few companies control the type of data necessary to compete effectively, and each firm does not license the data to others, then the merger may soften competition"[185].

Fourth, the Commission had a limited view about Facebook controlling so much data. Any privacy-related concerns was not considered to fall within the scope of the EU competition law rules but within the scope of the EU data protection rules.[186] This missed an important issue: was consumers' welfare at risk if Facebook started collecting and using data from WhatsApp's database? According to the European Commission officials the approach adopted was consistent with the statement by the Court of Justice of the European Union (CJEU) in the *Asnef-Equifax* case: "any possible issues relating to the sensitivity of personal data are not, as such, a matter for competition law, they may be resolved on the basis of the relevant provisions governing data protection".[187] The CJEU never provided any analysis for this statement.[188]

A fifth problem with the *Facebook/WhatsApp* decision involves the assumption of consumers readily detecting quality degradation. In addressing the likelihood of consumer lock-in, the Commission assumed that consumers could readily detect the exercise of market power post-merger and switch to rivals. This may be true post-merger for a price increase or a deterioration of the performances, not for privacy protection. It was not explored whether competition along this important parameter would likely diminish post-merger, and whether it would be likely to assist to a relevant switching migration by consumers.

Finally, it is hard to figure out under the Commission's analysis why Facebook acquired WhatsApp. Under neoclassical economic theory, companies merge for efficiencies and/or market power. Facebook paid USD 21.8 billion (USD 4 billion of which in cash) to acquire a company that in 2013 earned only USD 10.21 million in revenues, suffered a net loss of USD 138.146 million and did not amass a lot of user data. For the Commission, the "purchase price is not a parameter for determining the likely effects of a transaction on competition"[189], but it is legit to wonder why Facebook paid so

[185] Grunes A.P and Stucke M.E., (2016), supra, p.80

[186] European Commission, supra n 170, para 164

[187] In 2015, the same three Commission officials who mentioned the Asnef-Equifax case, elaborated how the degradation in privacy protections could violate competition laws: "a website that, post-merger, would start requiring more personal data from users or supplying such data to third parties as a condition for delivering its 'free' product could be seen as either increasing its price or as degrading the quality of its product. In certain circumstances, this behaviour could arguably amount to an infringement of competition law (irrespective of whether or not it also constitutes an infringement of data protection rules)". Ocello et al, supra n 121, p.6.

[188] Alec J Burnside, 'Setting the Scene', Paper presented at Antitrust, Privacy & Big Data: A Conference Organized in Partnership with Concurrences, 3 February 2015, p. 3

[189] Ocello et al, supra n 121, p.1

much for a company losing so much money. The perspective of efficiencies seemed unlikely[190], since Facebook promised to run WhatsApp separately, and significant technical hurdles were supposed to prevent the integration of the two databases. If efficiencies were not driving the merger, there still had be a sustainable competitive advantage deriving from the transaction. The Commission predicted that it would not. Moreover, if the market, despite the high market shares, had low entry barriers, little likelihood of market power from network effects, and a small, if any, data-advantage – as depicted by the Commission - is puzzling why Facebook spent so much for such a little competitor. The Commission never analysed the acquisition as a defensive mechanism aimed to block competitors from reaching the scale needed to compete effectively. Did the addition of WhatsApp amplify the data-driven network effects (making it harder for another firm to displace Facebook)? Facebook could continue to harvest data with its popular texting service, while WhatsApp represented a barrier to prevent threats from rival privacy-focused texting apps.

12.5 The case as a natural experiment

The Facebook/WhatsApp merger is an interesting case to deal with because it constitutes a sort of (partly) failed natural experiment. We have already mentioned that, In light of the prominent role played by personal data in the Commission's assessment, the Facebook/WhatsApp merger has been referred to as 'the vanguard of the analysis of data-driven mergers in multisided markets, where the product or service is free'.[191] Yet this view has been at least partially called into question, because of a proved degradation of WhatsApp services across the years finally ending up with a change in privacy-policy terms, which happened less than two years after the merger.

Under Facebook's control, WhatsApp's reputation for privacy quickly diminished. In 2015, WhatsApp received negative privacy marks (worse than its owner's ones)[192]. The Electronic Frontier Foundation criticized WhatsApp for not publicly requiring a warrant before giving content to law enforcement, not publishing a transparency report, not informing and providing notice to users about government data demands, and not publishing information about its data retention policies, including retention of IP addresses and deleted content.[193] In 2015, two security breaches were reported: hackers without a WhatsApp account could monitor the activities of the app users even if they turned on the privacy settings, and a security flaw enabled others to see users' profile photos even if they set it to 'Contacts-only'.[194]

Given the above-mentioned statement by the Commission about the privacy-sensitiveness of WhatsApp users, one would have expected them to promptly switch after these events. Instead, Facebook's dominance in texting has further increased. When the deal was announced, WhatsApp had 450 million users worldwide. By the time the Commission announced its decision, WhatsApp had 600

[190] Indeed, the word 'efficiency' does not appear in the Commission's decision.
[191] Stucke M. E and Grunes A. P., (2016), *Big data and competition policy,* Oxford University Press, p.79
[192] Andy Greenberg, 'Rating Tech Giants on Privacy: Google Slips, WhatsApp Fails', *Wired*, 18 June 2015, http://www.wired.com/2015/06/rating-tech-giants-privacy-google-slips-whatsapp-fails/
[193] Electronic Frontier Foundation, *Who Has Your Back? Fifth Annual Report on Online Service Providers' Privacy and Transparency Practices Regarding Government Access to User Data*, 17 June 2015
[194] Tech2 News, 'WhatsApp Security Flaw Allows Anyone to Track You Regardless of Your Privacy Settings', 13 February 2015, https://www.firstpost.com/tech/news-analysis/whatsapp-security-flaw-allows-anyone-to-track-you-regardless-of-your-privacy-settings-3662593.html

million users. By late 2015, WhatsApp had over 900 million active monthly users, more than the second-place Facebook Messenger (which had around 700 million active monthly users).[195] According to Facebook's CEO, 'numerous ways of monetizing the app will present themselves once it clocks 1 billion users'.[196] That occurred in early 2016, along with Facebook reporting that it was exploring new business models for WhatsApp to 'allow organizations to communicate with individuals with the user's consent'.[197]

The merged entity's conduct belied the Commission's predictions. As a natural experiment, the merger provides the empirical evidence that the Commission's analysis committed an assessment error with respect to the merging parties' incentives to combine their previously separate datasets. This brings us to some questions: Did the Commission get its analysis wrong? Could it have been aware of merged entity's incentives to integrate Facebook's and WhatsApp's databases post-merger? How can the Commission's error be explained?[198] The most straightforward and immediate explanation is that the Commission trustfully relied on the merging parties' misleading information denying the technological feasibility of the operation[199]. However, under the "even if" part of the investigation, any anticompetitive effect on the online advertising market was excluded even within the hypothesis of a matching of the data. Therefore, we can safely assume that Facebook's misleading information was not the reason for the Commission's assessment error.

In the next chapter we will support the idea that the Commission's error can be explained by its failure to fully assess the economic role of personal data in the evaluation of anticompetitive harm[200]. Indeed, the Commission never considered whether the matching of the companies' databases and the change in WhatsApp's privacy policy would have caused consumer harm on the consumer communications market. Taking into consideration the economic and strategic role of personal data would have enabled the Commission to accurately assess the incentives to integrate the parties' datasets. In addition, a privacy-related theory of harm would also have revealed the potential anticompetitive effects to the free side of the platform. While no likely competitive harm was identified on the online advertising market, the Commission simply omitted to assess potential harms on the consumer side[201].

12.6 A new perspective on the case

The intersection between privacy and data protection remains a complex matter in the antitrust and merger analysis. Even if the role of personal data as potential source of market power has been regularly recognized, competition authorities so far turn a blind eye to privacy-related consumer

[195] 'How Popular is WhatsApp?', http://www.whatsappfor.org/facts/popular-whatsapp-world/

[196] 'WhatsApp Has 900 Million Users, Closer Than Ever to a Real Business Model', *NeuroGadget*, 28 September 2015

[197] Natalia Drozdiak, 'WhatsApp to Drop Subscription Fee', *Wall Street Journal*, 18 January 2016

[198] Deutscher E., (2018), How to measure privacy-related consumer harm in merger analysis? A critical reassessment of the EU Commission's merger control in data-driven markets. in *Competition Law for the Digital Economy.* ASCOLA Competition Law Series, Edward Elgar, p.8

[199] See Ibid; and European Commission, 'Press Release - Commission alleges Facebook provided misleading information about WhatsApp takeover' http://europa.eu/rapid/press-release_IP-16-4473_en.html

[200] This is also the thesis supported by Deutscher E. (2018), supra.

[201] Deutscher E., (2018), supra

harm[202]. The explanation for this absence of a clear privacy-related theory of antitrust harm lies with the orthodox assumption we have already mentioned when we treated the Commission's decision[203]: privacy is not considered as an antitrust concern but should be properly addressed by consumer protection or privacy legislation.[204]. This view, is, however, increasingly being challenged by academics and by the Commission's subsequent enforcement practice itself[205].

While antitrust commentators and authorities have identified several data-related theories of harm, they exclusively focus on the role of personal data as a source of market power and anti-competitive foreclosure. All these foreclosure theories mostly locate the anticompetitive harm on the paying customer side of multisided platforms, causing indirect consumer harm whenever there are anti-competitive mark-ups on the advertising side. Scholars and antitrust authorities have not assessed to what extent the accumulation of personal data might also negatively impact consumers on the 'free' user side of online platforms[206]. There are potentially three approaches to include privacy in an antitrust investigation that solve this contradiction: privacy as a quality parameter, privacy as consumer choice and privacy as a non-monetary price. The latter is the one less implemented.

Privacy as a quality parameter

Both EU and US antitrust authorities underlined the importance of non-price parameters of competition, such as product quality, for their merger analysis[207]. However, so far, thy have been reluctant to block a merger on the sole ground of its negative impact on product quality or on other parameters of non-price competition.[208] In addition to this, the relationship between privacy and other factors of product quality is ambiguous, because a wider access to user data may enable to improve the overall quality of a product. The additional problems of subjectivity, multi-dimensionality and quantifiability make quality parameters very difficult to employ in antirust cases.

Privacy as consumer choice

A second way to include privacy in competition law analysis is framing privacy as an element of consumer choice. This consumer choice approach has been endorsed by the EU Commission in the Microsoft/LinkedIn merger. This approach, while being useful to identify privacy-related consumer harm deriving from vertical or conglomerate foreclosure effects, is not as efficient in the case of horizontal mergers. A horizontal merger brings a reduction of consumer choice only if the acquired and acquiring parties are close competitors. This is reflected in Facebook/WhatsApp where the Commission held that the merger was unlikely to harm competition on the consumer communications services market because the merging parties were not considered as close substitutes.

---

[202] Deutscher E., (2018), How to measure privacy-related consumer harm in merger analysis? A critical reassessment of the EU Commission's merger control in data-driven markets. in *Competition Law for the Digital Economy.* ASCOLA Competition Law Series, Edward Elgar

[203] See page 48, point four of our discussion of the European Commission's decision

[204] Maureen K Ohlhausen and Alexander Okuliar, 'Competition, consumer protection, and the right (approach) to privacy' (2015) 80(1) Antitrust Law Journal 121 151 ff; This assumption has been expressly endorsed by the FTC, the EU Commission and the Court of Justice of the European Union in European Court of Justice]

[205] Deutscher E., (2018), supra note 190

[206] Ibid, p.10

[207] Kimmel L. and Kestenbaum J., (2014), 'What's Up with WhatsApp? A Transatlantic View on Privacy and Merger Enforcement in Digital Markets', 29(1*) Antitrust* 48 53

[208] Stucke M. E and Grunes A. P., Big data and competition policy*,* Oxford University Press, 2016, p. 115.

Privacy as a non-monetary price

There is a third route to incorporate privacy into competition analysis: the conceptualization of personal data disclosure as a non-monetary price which users pay to have free goods and services [209]. The intuition that privacy constitutes the real price consumers in online markets is theoretically based on the concept of 'privacy calculus' which we already considered in chapter 9. If one accepts the intuition that personal data are the price for free online services, a decrease in privacy is to be considered as equivalent to an increase in price.[210] Framing privacy as a non-monetary price would expand the toolbox of merger control in data-driven markets when defining relevant markets and when assessing the harm to consumers.

12.7 Privacy-price as a new tool for market definition

The insight that privacy constitutes a non-monetary price for data-driven services might enable competition authorities to deal with the challenges posed by market definition in online multi-sided markets with zero-priced products. These challenges are two-fold. On the one hand, in several cases competition authorities and courts failed to account for the interdependencies between the different market-sides of multisided platforms, focusing only on their paying, advertising side, while ignoring the free, user side.[211] On the other hand, zero-pricing adds another element of methodological complexity to market definition in the online eco-system. The conventional method used, the Small but Significant and Non-Transitory Increase in Price (SSNIP) test, is not reliable for markets where goods are provided for free, and price is not the most important parameter of competition[212]. A suggested solution to this complexity is to define markets accounting for the role of personal data on both market-sides of a multisided platform[213]. To this end, privacy can be the proxy to substitute monetary prices as a tool for market definition. Data market could be defined by testing users' response to a Small, but Significant and Non-transitory Decrease in Privacy (SSNDP test)[214]. The SSNDP test is based on the idea that consumers barter the disclosure of personal data in exchange for free services, but unfortunately it is still not easy to make it operative.

In the market definition of Facebook/WhatsApp case, the Commission did not define any separate product market for personal data, since Facebook did not sell any data or data-analysing services and

[209] Gal M. and Rubinfeld D., (2016), The Hidden Costs of Free Goods: Implications for Antitrust Enforcement, *Antitrust Law Journal* (80) 3, 542.; John M Newman, (2015), 'Antitrust in Zero-Price Markets: Foundations', 164 U. Pa. L. Rev. 149 173.; Magali E., (2016), 'How Free Internet Services Challenge Traditional Antitrust Tools: Personal Data as a Price', 11–33; Grunes P.A and M. E Stucke, 'No Mistake About It: The Important Role of Antitrust in the Era of Big Data' [2015] *University of Tennessee Legal Studies Research* Paper No. 269, 4–6; Stucke, M. E. and Ezrachi A., (2015), 'When Competition Fails to Optimise Quality: A Look at Search Engines', *University of Tennessee Legal Studies Research* Paper No. 268, 36

[210] Ezrachi A. Stucke M. E., *Virtual Competition: The Promise and Perils of the Algorithm-Driven Economy*, Cambridge, MA: Harvard University Press, 2016; Bundeskartellamt/Autorité de la Concurrence (2016), *Competition law and data*.

[211] Harbour, 'Dissenting Statement of Commissioner Pamela Jones Harbour in the Matter of Google/DoubleClick F.T.C. File No. 071-0170' (n 9) 7

[212] Gal M. and Rubinfeld D., (2016), The Hidden Costs of Free Goods: Implications for Antitrust Enforcement, *Antitrust Law Journal* (80) 3, 542

[213] Harbour, 'Dissenting Statement of Commissioner Pamela Jones Harbour in the Matter of Google/DoubleClick F.T.C. File No. 071-0170' (n 9) 4

[214] Stucke M. E and Grunes A. P., (2016), *Big data and competition policy,* Oxford University Press, p.118–122

WhatsApp did not collect them for advertising purposes. By exclusively focusing on whether personal data was sold or used as an input on the advertising side of the merging parties, the role of privacy as non-monetary price on the free consumer side was overlooked. The Commission's approach replicated the error generally occurring when market definition exclusively focuses on the paying side of a multisided platform[215]. The paying and free market sides of the merging multisided platforms were assessed in isolation and under the prism of price increases[216]. This resulting market definition underestimated the spillover effects between the advertising and the consumer side of the market. Yet, it is exactly these cross-platform effects which motivated the integration of Facebook's and WhatsApp's databases. The integration was considered by the Commission as a self-defeating strategy. This conclusion, however, rested on the erroneous assumption that a change in WhatsApp's privacy policy would have induced consumers to switch to competing apps. This would have entailed negative spillovers on the online advertising side, which would have brought even more losses to the merged entity[217]. In a multisided platform environment, a price increase indeed triggers that kind of spillover effect, but this is not necessarily true in the case of privacy-price increases. A decrease in the protection of privacy will not necessarily lead to a decrease of the platform's attractiveness for advertisers. It might instead make the platform even more attractive because of its increased access to a wider dataset of personal information.

12.7.1 Privacy-price as an analytical basis for a theory of privacy-related consumer harm

The conceptualization of personal data as a non-monetary price allows to formulate a theory of harm potentially useful for enforcers' merger analysis. The concept of privacy-price points to a more immediate form of consumer harm on the free user side than the usual indirect harm following dat-driven foreclosure. It makes possible to formulate a decrease in privacy protection resulting from a merger as a reduction in consumer welfare similar to a price increase. We will see in Chapter 13 that a similar theory of direct privacy-related harm has been recently articulated by the Bundeskartellamt, the German competition authority.

A similar theory of harm could inform and complement the unilateral effects analysis in horizontal mergers, beyond the parameters of price or quality[218]. The competition authority could determine to what extent the merger increases the merged entity's ability and incentive to deteriorate the level of privacy[219]. Such would be the case if the merged entity could internalize part of the users losses due to degradation of privacy protection, by capturing part of these users with the previously independent close competitor[220]. The privacy-price concept thus allows to integrate privacy in the upward pricing pressure test in horizontal merger cases. Such unilateral effect analysis can also account for "strategic complementarity" effects post-merger: how do competitors react to the merged entity actions in terms of privacy standards? Such a privacy-related theory of consumer harm would have enriched the

[215] Deutscher, supra, p.15
[216] Ibid
[217] Ibid.
[218] Ibid, p.16
[219] In the Dow/Dupont Merger the Commission applied such a theory of harm of unilateral effects analysis to assess the merger's effect on the non-price parameter of innovation. Case COMP/M.7932 Dow/DuPont (n 82) [2000] - [2020].
[220] See in this sense Merger Guidelines 2010 (n 80) 21. Commission Guidelines on the assessment of horizontal mergers (n 80) [24].

Commission's analysis in the Facebook/WhatsApp merger in several respects[221]. In its assessment, the Commission didn't formulate a specific theory of harm on the consumer communication market, omitting to justify why was looking for a price increase or a decrease in quality. Based on the concept of privacy-price, the commission might have looked for a likely increase of the collection of personal data on the consumers' side of the market. This could have been the main object of the unilateral effect analysis on that side.

Second, such theory of harm would have allowed a better understanding of the closeness of competition between Facebook and WhatsApp. The Commission found the parties to be complementary[222] rather than substitutes because of different functionalities, different privacy policies and multi-homing practices by users[223]. The investigations were conducted only on a quality dimension, it was never assessed the extent to which WhatsApp was constraining Facebook through its higher degree of data protection.

Third, as we already explained above, a privacy-price theory of harm would have revealed the merged entity's incentive to match the parties' datasets and lower WhatsApp's privacy protection post-merger. The acquisition allowed Facebook and WhatsApp to profitably lower their privacy protection. The Commission did not attribute enough weight to direct network effects being the source of consumer lock-in and status quo bias, defeating the countervailing effects of multi-homing and low switching costs. The parties' incentives to merge the datasets were reinforced by the gains in advertising revenues, due to the internalization of spillover effects between different sides of the platform.

Finally, thanks to a privacy-related theory of harm the Commission might have assessed the extent to which WhatsApp was seen as a maverick in the consumer communications services market and as a potential competitive threat to Facebook's core business in the social networking market. Before the merger, in most EU countries,[224] WhatsApp had changed its business model from a subscription-based to a free-of-charge provision of its app, without collecting more data or introducing ads. In the long term, this could have undermined Facebook's user-data- and advertising-driven business model.

Before concluding the chapter and passing to the next and more recent case involving Facebook, we would like to briefly mention two different tools to analyse the competitive role of privacy in antitrust cases. The first one was published by Keith Waerher[225], the second one by Elias Deutscher and is directly based on the concept of privacy as non-monetary price[226].

[221] These are explained by Deutscher in his paper.
[222] Case COMP/M.7217 Facebook/Whatsapp (n 2) [106]
[223] Ibid 102-105
[224] Except in UK and IT where it charged an annual fee of 0,89 EUR
[225] Keith Waehrer, 'Online Services and the Analysis of Competitive Merger Effects in Privacy Protections and Other Quality Dimensions', Working Paper, 12 January 2016
[226] Deutscher E., (2018), How to measure privacy-related consumer harm in merger analysis? A critical reassessment of the EU Commission's merger control in data-driven markets, *Competition Law for the Digital Economy.* Edward Elgar, (ASCOLA Competition Law Series).

12.7.2 Downward quality pressure

Economist Keith Waehrer elaborated a model to analyse the competitive effects deriving from a merger between online services competing on the level of privacy protection offered to consumers[227]. The method proposed allows to quantify the non-price effects of a merger (including privacy) with a procedure similar to the one already used to quantify upward pricing pressure[228]. Waehrer's approach seeks to help the agencies avoid the likely subjectivity, measurement, and multi-sided platform pitfalls. Assuming that consumers value some degree of privacy (which appears to be empirically supported, even if the monetary estimation of data by the subjects still proves to be difficult. We treated these issues in chapter 9), Waehrer observes that some degree of privacy protection makes services more attractive to users. However, even if there is a certain competition on this parameter, the firms still generally prefer lower levels of privacy protection. Privacy protection is costly to provide and it also affects the revenues a firm makes through targeted advertising or the sale of consumer information. Thus, firms make a trade-off in deciding how much privacy protection to offer in order to attract or retain users to their 'free' online services.

Waehrer bases his model on a hypothetical set of facts, which can be applied to several real-world online mergers. The main assumption is that the advertising side of the market remains competitive after the merger. This is useful for two reasons. First, if a merger brings higher market power in the advertising market, the agencies already have tools available to tackle the issue. Second, and importantly, taking this assumption as true, then a loss of consumer privacy would not be protected by looking solely at the advertising side. Given that many online services in which privacy is an issue are priced at 'zero' on the consumer side, it is not likely to expect price effects from a merger on the consumer side, even when the services appear to be close substitutes. Pricing to consumers is therefore constrained, and this is well corroborated by the reality. Online companies rarely charge 'negative' prices or charge consumers a small amount for the use of the service. When price is constrained, it is widely acknowledged that quality competition becomes more important[229].

Thus, Waehrer derives a formula[230] for assessing downward quality pressure, assuming some loss (diversion) of users in response to lower privacy protection, and that the merger would allow the merged firm to recapture some of these users. In that way, a firm can profitably lower privacy protection unilaterally post-merger. This is analogous to the unilateral effects analysis already used by antitrust enforcers. The model takes efficiencies into account, does not require the actual measurement of privacy (or quality more broadly), and has unambiguous results. If certain conditions are satisfied, a merger between two online advertising-supported firms may lead to a reduction in

[227] Keith Waehrer, (2016), 'Online Services and the Analysis of Competitive Merger Effects in Privacy Protections and Other Quality Dimensions' https://www.researchgate.net/publication/314545798_Online_Services_and_the_Analysis_of_Competitive_Merger_Effects_in_Privacy_Protections_and_Other_Quality_Dimensions

[228] US Horizontal Merger Guidelines, above note, s 6.1; *see also* Joseph Farrell and Carl Shapiro, 'Upward Pricing Pressure and Critical Loss Analysis: Response', *CPI Antitrust Journal* (February 2010)

[229] *Microsoft/Skype* (Case Comp/M.6281), Commission Decision C(2011)7279, 7 October 2011, para 81 (noting that '[s]ince consumer communications services are mainly provided for free, consumers pay more attention to other features' and '[q]uality is therefore a signifcant parameter of competition'); *Microsoft/Yahoo! Search Business* (Case Comp/M.5727), Commission Decision C(2010) 1077, 18 February 2010

[230] Keith Waehrer, Ibid, p. 14-17

consumer welfare. To sum up, this paper is an important step in providing new tools to enforcers in the era of Big Data.

12.7.3 Conjoint analysis

The model by Elias Deutscher[231] relies on the concept of 'privacy calculus'. The operative contribution by the author (built on the concepts explained in the chapter above) is the use of willingness-to-pay studies in the form of conjoint analysis. This tool would enable competition authorities to quantify privacy-related consumer harm in monetary terms, balancing it with potential welfare-enhancing efficiencies.

Initially developed by the marketing literature, conjoint analyses are widely used as an instrument to identify how certain features of a differentiated product are valued by consumers and, thus, influence consumers' choices and willingness to pay[232]. To this end, conjoint analysis models identify the respective value of specific product attributes (the so called 'part-worths') for consumers' overall utility[233], by measuring how changes in these attributes influences consumers' preferences.

Conjoint analysis relies on economic experiments in the form of choice-tasks, which confront them with 'hypothetical, but realistic choice problems' in the form of different variations or profiles of a given product (so-called 'stimuli')[234]. It thus tries to mimic situations that consumers face in the market place, rather than relying on consumers' stated preferences. The analysis is done in three steps. The first one is basically a consumer survey, necessary to individuate the relevant attributes for a given product[235]. In the Facebook/WhatsApp case, the Commission could have identified the product attributes and attributive levels for the consumer communications apps set out in Figure 6[236]. In a second step, the competition authority could design different profiles (stimuli) of the product, by bundling varying attributes and attributive levels. In the third step, a representative[237] sample of consumers would be confronted with a limited number (ideally 12-20) of paired choice tasks and asked to rank the product profiles according to their preferences by allocating a fixed sum of points (e.g. 100 points).

---

[231] Deutscher E., (2018), How to measure privacy-related consumer harm in merger analysis? A critical reassessment of the EU Commission's merger control in data-driven markets. in *Competition Law for the Digital Economy.* ASCOLA Competition Law Series, Edward Elgar

[232] For the economic foundations of the conjoint analysis Paul E Green and Vithala R Rao, 'Conjoint Measurement for Quantifying Judgmental Data' (1971) 8(3) Journal of Marketing Research 355

[233] McFadden, 'The Choice Theory Approach to Market Research' (n 127) 279; Paul E Green, Abba M Krieger and Yoram Wind, 'Thirty Years of Conjoint Analysis: Reflections and Prospects' (2001) 31(3_supplement) Interfaces 56; Green, Krieger and Wind (n 128), 59–60.

[234] Stephen Hurley, 'The Use of Surveys in Competition and Merger Analysis' (2010) 7(1) Journal of Competition Law & Economics 45 63

[235] Arguably, this exercise is already part of the competition analysis in mergers, as the competition authorities have to determine the product features and specificities for the product market definition. Case COMP/M.7217 Facebook/Whatsapp [13] - [33].

[236] Gergely Biczók and Pern H Chia, (2013), 'Interdependent Privacy: Let Me Share Your Data' in David Hutchison and others (eds), *Financial Cryptography and Data,* Springer Berlin Heidelberg; Yu Pu and Grossklags J., 'Using Conjoint Analysis to Investigate the Value of Interdependent Privacy in Social App Adoption Scenarios: Research Paper presented at the 36th International Conference on Information Systems, Fort Worth 2015' (2015) 2.

[237] n = ideally around 1000, the sample should represent different age and population groups and should be composed by existing and future consumer communications app users.

Attribute	Attributive Level
Price	• free (0 €) ;or • paying (1,99 €)
Network popularity	• 5% of friends/contacts using the same app • 25 % • 50% • more than 50%
Number of communication parties	• one-to-one and/or • group chats
Functionalities	• text • photo • voice messaging • video messaging • video chat • group chat • voice call • sharing of location and other information
Availability	• only on one operating system (proprietary app) • or multiple operating systems (cross-platform apps)
Platform compatibility	• only smartphone • all mobile devices • all electronic communication devices
Privacy	• no disclosure of personal information, • disclosure of a basic profile (name plus additional identifier (i.e. email address or phone number) • full profile • profile of contacts and friends (interdependent privacy)[137]

Figure 6 - Product attributes and attributive levels of consumer communications services[238]

On the basis of the overall utility ranking of different profiles by the respondents, the agencies could estimate the utility and relative importance of each attribute and attributive level for the consumers' product choices by means of multi-variable regressions. The quantification of a parameter like privacy can be done by weighting the changes in utility due to variations in the attributive level with the utility changes in response to changes in monetary prices. Thus, the competition authority could gauge how much consumers are willing to pay for a certain level of a non-price attribute of the product, such as privacy.

Conjoint analysis may inform the definition of a 'data market' by indicating which change in the level of privacy corresponds to a small but significant and non-transitory increase in price (usually 5-10% price increase)[239]. In the case of merging parties invoking merger specific efficiencies, the conjoint analysis may enable authorities to balance the consumer harm arising from a decrease in privacy with pro-competitive efficiencies.

[238] Deutscher E., (2018), supra note 216, page 22
[239] For the use of conjoint analysis for market definition see Hildebrand (n 132), 327–334.

Conclusion

We mentioned these two approaches above to show how the research is already proposing methods to deal with privacy as a competition parameter which are consistent with the theoretical framework we have adopted so far. Both have the merit of formulating a direct harm on the consumer side and of offering practical and applicable tools. Currently, the antitrust assessment of privacy is still very difficult from an operative point of view. The antitrust agencies' investigations are not only complicated by the non-price/quality dimension of privacy, but also by the general innovative and fast-developing nature of the online eco-system. In the last decade, the European Commission has been particularly sensitive to the competitive dynamics in the digital markets, but it is common opinion that the toolbox employed since now needs an update to face the new challenges[240]. In the next chapter, we discuss a recent case that goes in a direction never adopted before by enforcers. As we will see, for the first time the violation of data protection was considered as directly dependent from a position of dominance in the market. After analysing the case, we will see which are the unprecedent potential implications of this decision on the activity of both the authorities involved.

13. The Bundeskartellamt's vanguard decision. Case B6-22/16

In this last and conclusive chapter, we would like to treat the case which is currently at the frontier of competition law applied to matters of data protection and privacy. We could define it as 'vanguard' not only because of the timing (the first documents were released on February 2019, after three years of investigations), but especially because this is the very first case in which a competition agency detected and then fined an abuse of dominance achieved by a practice commonly under the exclusive jurisdiction of data protection authorities. The case is very fresh, and very hotly debated and criticized. We will mention opposite opinions about its validity and methodology, trying to account for the overall complexity of the issue rather than individuate a solution. This is probably too early to do, and way beyond our capacity. The decision is clearly at the intersection between competition law and data protection, it is coherent with the reflections and concepts we developed until now and, finally, it is a new frontier of the antitrust enforcement.

13.1 Bundeskartellamt's decision on Facebook

In July 2019, Germany's Federal Cartel Office (from now on "FCO") published its decision on the Facebook case. The decision qualifies 'as an abuse of dominance the Facebook's current practice of collecting and matching data of its users from third-party services/websites without explicit consent[241]'.

[240] This exigence was also confirmed by the last report wanted by incumbent Commissioner Margrethe Vestager. See European Commission, *Competition Policy for the digital era: Final report*, April 2019

[241] See Heinz Silke, Bundeskartellamt hits „don't like"-button on Facebook, *Kluwer Competition Law Blog*, February 11 2019. Available at: http://competitionlawblog.kluwercompetitionlaw.com/2019/02/11/bundeskartellamt-hits-dont-like-button-on-facebook/

The third-party sources are data generated, on the one hand, by the use of services owned by Facebook, such as e.g. WhatsApp and Instagram; on the other hand, by the use of third-party websites and apps outside of Facebook services. If a third-party website has embedded the so-called "Facebook Business Tools": the "Like" button, "Facebook login" or analytical services such as "Facebook Analytics", data are transmitted to Facebook via APIs (Application Programming Interface) when the user navigates that third-party website for the first time. In accordance with Facebook's terms and conditions, these third-party data can be combined with data from the user's social network account and used by Facebook, even if users have blocked web tracking in their browser or device settings. So far, users have been able to use the social network only under these conditions. Otherwise, it is not possible for them to register. In the authority's assessment, these terms and conditions are neither justified under data protection principles nor are they appropriate under competition law standards. The authority's decision covers differently the third-party data sources[242]:

i. Facebook-owned services like WhatsApp and Instagram can continue to collect data, whereas assigning the data to Facebook user accounts will only be possible subject to the users' voluntary consent. Where consent is not given, the data must stay with the respective service and cannot be processed in combination with Facebook data.

ii. Collecting data from third-party websites and assigning them to a Facebook user account will only be possible if users give their voluntary consent. If consent is not given for data from Facebook-owned services and third-party websites, Facebook will have to substantially restrict its collection and combining of data.

The FCO concluded that Facebook's conduct violated the EU data protection laws (General Data Protection Regulation – GDPR)[243], by violating the human right to control the processing of personal data and the constitutional right of informational self-determination. Most importantly, it also stated that Facebook's dominant position was a key element of such privacy violation: establishing a link between the antitrust element of market power and the traditional privacy issues connected to information disclosure. This is the core of the decision. Let see briefly how the assessment was carried on and which are the methodological justifications of the FCO.

13.2 Market definition and dominance in the German social networks market

The FCO defines a separate digital social networks market in Germany[244]. Other online services like professional networks (LinkedIn and Xing), messaging services (WhatsApp and Snapchat) or other social media (YouTube or Twitter) are not found to be in the same market, because they largely satisfy complementary needs in terms of functionalities. We have seen in the WhatsApp case that competitive constraints can be present also in a situation in which two competitors offer complementary functionalities. So, it would probably be more accurate to assess this market definition in terms of demand substitutability. The above-mentioned online services are not considered as close substitutes because they don't offer the same kind of social experience and, indeed, users are not willing to switch

[242] Directly reported from Bundeskartellamt's Press release, p.1. Accessible at: https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html;jsessionid=CD992BC966DC64354F5382649309F635.1_cid378?nn=3600108

[243] Regulation (EU) 2016/679, (2016) OJ L 119/1

[244] Bundeskartellamt, *Decision B6-22/16*, 2019, para 344

between them. According to the FCO's decision, even if these competitors were included, Facebook's market share would still be indicative of dominance, since it would exceed the 40 percent, which is the threshold set by German law. Almost all the other online services with the highest user numbers belong to the Facebook group and the decision reports that 'even if WhatsApp were to be excluded from the market, as claimed by Facebook[245], Facebook would still achieve a very high share of daily active users with its services Facebook.com and Instagram'.

The market is limited to Germany because it was found that German consumers mainly use Facebook to keep in touch with other users in Germany. The company has a dominant position for social networks with 23 million daily active users and 32 million monthly active users, corresponding to a market share of more than 95%[246] (daily active users) and more than 80% (monthly active users)[247]. The market power assessment is not only based on the estimation of market shares. In accordance to the German competition act, other relevant factors were considered[248]: the access to competitive relevant data, the economies of scale based on network effects, the behaviour of users (a considerable lock-in situation was found[249]), and the power of innovation-driven competitive pressure. All these criteria provided proof of Facebook's market power. The company position is strengthened by direct and indirect network effects. A new competitor must achieve high critical number of private users to be able to offer a rival competitive ad-financed product. Without such critical number, the product is not enough attractive for the advertising side. However, direct network effects make it difficult to achieve such threshold of users in the first place. Considering all these factors and consumer behaviour (multi-homing practices couldn't be established by the authority), FCO defined high entry barriers.

13.3 Theory of harm: abusive terms and conditions

The theory of harm is that Facebook abuses its dominant position through the imposition of abusive exploitative terms and conditions to users. The FCO primarily relied on the German case-law, according to which the violation of legal principles (including civil law) can make business terms abusive.

The FCO finds the terms and conditions abusive, since they violate data protection laws making the use of the social network pre-conditional upon vast data collection and combination. The data collected across third-party websites by the "Facebook Business Tools", are matched and processed together with the users' social network accounts. Users do not even have to really click on the embedded APIs (application programming interfaces, i.e. "Like-Button and "Share-Button"), navigating such sites is enough to be tracked. All these procedures occur in presence of unaware users who did not give their explicit consent. Therefore, the FCO judged the situation as in violation with EU Data protection laws.

[245] Paragraph 409 and 420 of B6-22/16 decision
[246] Facebook has 2.3 billion monthly active users worldwide of which 1.5 billion on a daily basis.
[247] Bundeskartellamt, *Press release* p.2
[248] B6-22/16 decision, paragraph 422
[249] In particular, it was established that, due to this market position, Facebook's users cannot switch to other social networks with minimal effort or an equal level of satisfaction.

In the balancing of interests exercise[250], required under German law, the FCO states that 'there is a gross imbalance between the interests of Facebook, only some of which are legitimate, and the protection of users' fundamental rights when processing data from Facebook-owned services and Facebook Business Tools, especially when a holistic view is taken'[251]. Facebook practices are inappropriate and not necessary for the provision of the social network services. In addition, users have no choice to opt out even when aware: it is a take it or leave it situation. The user interest to have control over their data and the fundamental right of so-called informational self-determination were weighted as more important than Facebook's interests.

13.4 The interpretation of GDPR by the competition authority

If we want to analyse the Facebook decision in light of the EU data protection rules, it is necessary to remind of a core principle of the GDPR: processing personal data is generally prohibited, unless either the data subject has consented to the processing (Article 6(1)(a)) or in some specific cases where the processing is expressly allowed by law (Article 6(1)(b-f))[252]. GDPR gives individuals full control of their personal data and recognizes them the right to decide whether or not to have their personal data processed. The basic requirements for a legally valid consent are defined in Articles 4 and 7 and specified further in Recitals 32, 42 and 43 of the GDPR. Consent is defined by Article 4 as 'any informed, specific, unambiguous, and freely given indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her'[253]. GDPR has also the intent of making data controllers accountable for their data processing activities, requiring them to perform some activities which guarantee that data subjects' consent, once granted, is well-grounded, genuine, and demonstrable[254]. It asks data controller to inform data subjects about its identity and the intended purposes of data processing (recital 42) and about the right to withdraw consent at any time (article 7(3)). In addition, the GDPR makes sure that data subjects grant an explicit consent and that they are aware of the exact extent of it (Recital 42). That's why processing activities related to different purposes needs separated consent (Article 7(2) and Recital 42). When consent is requested in a written declaration (formulated with a clear and plain language), all the matters involved must be distinguished, intelligible and accessible. Finally, the consent must be obtained without forcing or misleading the users. Particularly interesting for our discussion is that, according to Recital 32, consent is not considered as freely given where[255]:

(i) the data subject has no free choice or is unable to refuse consent easily and without detriment (Article 7(3) and Recital 42);

[250] Bundeskartellamt decision B6-22/16, para 870
[251] Ibid.
[252]Beyond consent, the GDPR mentions other five legal bases for data processing, that are: a contract, legal obligations, vital interests of the data subject, public interest and legitimate interest pursued by the controller or by a third party.
[253] General Data Protection Regulation, Article 4
[254] Colangelo G. and Maggiolino M., (2019), Antitrust Über Alles. Whither Competition Law After Facebook?, *World Competition Law and Economics Review*, 2019, 42(3
[255] Ibid, p.8

(ii) the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract (Article 7(4))

(iii) there is a clear imbalance between the data subject and the controller (Recital 43);

(iv) the data subject is prevented from giving separate forms of consent to different data processing operations (Recital 43).

In examining whether Facebook's data policy respected all these GDPR provisions, the FCO acted as if it were a data protection authority: users' consent was not considered as genuine nor freely given, and data practices not necessary to offer the social network service. Very important to notice here is that there is nothing in the GDPR that makes the quality of the consent dependent on the amount of market power of the data controller. The GDPR does not include anything similar to a 'special privacy responsibility' of dominant firms[256]. Once again, this is a new interpretation of the GDPR made in order to undermine Facebook's data accumulation strategy[257].

13.5 Privacy as antitrust injury

As seen above, Facebook's conduct caused a privacy harm, directly impacting consumers' welfare. Once it reached this conclusion, the FCO turned this privacy harm into an antitrust injury[258]. First of all, because competition is the proper FCO's jurisdiction, and secondly, because this appears to be the goal since the beginning: to target and limit the company data accumulation strategy.

To this end, the FCO stressed that Facebook's violation of the constitutional right to informational self-determination [259] is linked to its dominant position in the market. The FCO relied on the case-law of the German Federal Court of Justice, which recognizes an abuse of business terms whenever terms and conditions are applied as a manifestation of market power or superior bargaining power[260]. Notably, the case law is applicable to all other areas of the law presenting this unbalanced negotiation. In the name of this constitutional right, the FCO intervenes to prohibit unfair business terms imposed by one dominant party to the others. An additional motivation was that the conduct granted to Facebook a competitive edge and increased market entry barriers, which in turn has secured Facebook's market power over end users.

In summary, the Facebook decision has been taken under the German Competition Law, but the FCO used the data protection principles and rules mentioned in the previous paragraph as a benchmark to

[256] Ibid, p.9. True, as Recital 43 recalls, imbalance between data controllers and data subjects may call into doubt the freely given nature of the consent.
[257] The Bundeskartellamt proved even the non-compliance to all the subsections of Article 6 of the GDPR. See Case B6-22/16, paras. 716 – 719 for Article 6(1)(c) GDPR; paras. 720 – 722 for Article 6(1)(d); para 723 – 726 for Article 6(1)(e), and paras. 727 – 869 for Article 6(1)(f)
[258] Colangelo G. and Maggiolino M. (2019), supra note 239, p.10
[259] The right in the name of which data protection law provides individuals with the power to decide freely and without coercion on the processing of their personal data.
[260] Bundeskartellamt, Case B6-22/16, paras. 525-534; Bundeskartellamt, Case summary, *supra*

assess the abusive nature of the terms and conditions applied. The FCO did not categorize the conduct as an exclusionary abuse but as an exploitative one.

13.6 Unfairness and exploitative business terms: the Facebook's conduct under Article 102(a) TFEU

Since FCO has assessed an abuse of exploitative business terms, the appropriate legal reference would be Article 102(a) TFEU[261]. From this perspective, the theory of harm would formulate third-party tracking as an excessive data collection[262]. As we have seen in Chapter 12, in data-driven business models, the quantity of personal data exchanged for the platforms' services can be conceptualized as a non-monetary price. This conceptualization may justify the FCO investigation under Article 102(a) TFEU. According to this interpretation, data collection may end up being exploitative whenever the arrangements set under the terms and conditions are unfair. For instance, Facebook imposed to consumer an excessive price (in terms of personal data) through unfair terms and conditions possible only because of its dominant position. The notion of unfairness has only been analysed by the CJEU and the European Commission in a few decisions[263] . Some main circumstances have been identified: clauses which are unjustifiably unrelated to the purpose of the contract, unnecessarily limit the freedom of the parties, are disproportionate, unilaterally imposed or seriously opaque[264]. Therefore, considering all these factors, the FCO might have succeed to justify its decision under the European law, too. Furthermore, the Bundeskartellamt might have arrived at this conclusion even without giving any consideration to EU data protection law.

13.7 Conclusive remarks: the debate

In its decision of February 6, 2019, the FCO ordered significant changes to Facebook's data collection and usage practices[265]. If upheld on appeal[266], the decision promises to establish new standards for data collection and data usage at least for market-dominant undertakings.

---

[261] In the FAQ's document relasead by the Bundeskartellamt it is admitted explicitly that the investigation could have been possible even under article TFEU 102(a). The national law was chosen because stricter (as explained in paragraph 914 of the decision) and because it does not imply the risk that the case will be referred to CJEU (See M. Botta and K.Wiedemann, The Interaction of EU Competition, Consumer and Data Protection Law in the Digital Economy. The Regulatory Dilemma in the Facebook Odyssey*, Antitrust Bulletin)*

[262] See A. Ezrachi and V.H.S.E. Robertson, (2019), Competition, Market Power and Third-Party Tracking, 42 *World Competition* 5, 8-9 arguing that extensive data gathering and analysis in digital markets, in particular through combining data from multiple sources, has the capacity to support the creation of market power.

[263] H. Kalimo and K. Majcher, (2017), The Concept of Fairness: Linking EU Competition and Data Protection Law in the Digital Marketplace, *42 European Law Review 210*

[264] R. Nazzini, (2019), Privacy and Antitrust: Searching for the (Hopefully Not Yet Lost) Soul of Competition Law in the EU after the German Facebook Decision, *Competition Policy International* (2019), arguing that the EU case law and Commission practice are capable, in theory, of supporting a finding of abuse by a dominant social network if its privacy policy is unfair under Article 102(a) because it is disproportionate or has no connection with the purpose of the contract with the end user.

[265] At the time of the decision in February 2019, Andreas Mundt, President of the Bundeskartellamt stated: "With regard to Facebook's future data processing policy, we are carrying out what can be seen as an internal divestiture of Facebook's data. […]"

[266] According to the case summary published by the FCO, Facebook has already appealed against the decision; cf. FCO, *supra*, p. 12

The European Data Protection Supervisor (EDPS) Giovanni Buttarelli welcomed enthusiastically the FCO decision[267], as the first to finally integrate data protection implications into the antitrust remit. In his perspective, the case clearly evidences that European data protection provisions are deemed to be a standard for examining exploitative abuses. Overall, the decision has a pioneering potential, and marks an important step in looking at data protection rules as a benchmark for competition enforcement purposes[268]. The author's wish is the opening of a fruitful osmosis and synergy between the two agencies. He warned: "All companies in the digital information ecosystem that rely on tracking, profiling, and targeting should be on notice"[269].

Buttarelli also disagrees with some of those claiming that the mutual inclusion into each other's goals implies that data protection needs to resort competition law in order to achieve its purposes, and conversely, with others fearing that this osmosis of goals would "enslave" competition law to issues outside its remit.[270] For the Supervisor it is incorrect to approach this new relationship as a matter of supremacy, but it is rather an opportunity to adjust the authorities' toolbox and to empower the instruments already available. The enthusiasm in front of this vanguard and innovative case is comprehensible. However, it is impossible to hide (and it is naturally clear to Mr Buttarelli, too) that the convergence of privacy and competition law (with their respective enforcers) creates numerous dilemmas.

The implications of Bundeskartellamt's decision are thorny and raised a lively and complex debate. There are many aspects which need to be re-defined and clarified after the unusual and innovative approach adopted by the German authority. We will try to highlight the main topics and problems which are now discussed by scholars, agencies, lawyers and economists involved both in the antitrust and data protection sectors.

Without focusing on the details of the case, problems could generally derive by the auspicated convergence between different authorities and the unavoidable overlapping of their different interests and purposes. In the digital economy we can expect data protection, consumer protection, and competition frameworks to interact with each other to a certain extent. At the same time, these frameworks are not designed to address the same issues, and in some cases, they may be in tension with one another. For instance, a competition enforcer may wish to facilitate access to data to alleviate competition concerns, but such access may raise privacy concerns if the data includes personal information. On the other hand, privacy and consumer protection frameworks encouraging portability may alter the competitive significance of data by lowering barriers to entry. Striking the right balance depends on a case-by-case analysis of the facts.

Privacy law frameworks are effectively a slippery ground for competition agencies. Data protection law balances a number of aspects of data policy such as choice, transparency, control, access, portability, and correction, which competition tools are limited in addressing and may even be in tension with[271]. Can privacy and competition values live in harmony as friends, will some of these proposals make them

[267] G. Buttarelli, 'Big step towards coherent enforcement in the digital economy', (2019) https://edps.europa.eu/press-publications/press-news/blog/big-step-towards-coherent enforcementdigitaleconomy_en

[268] G. Buttarelli, *This is not an article on data protection and competition law*, CPI Antitrust Chronicle (2019)

[269] Ibid, p.11

[270] Ibid

[271] *CPI Talks with… Terrell McSweeny*, CPI Antitrust Chronicle, February 2019

enemies, or is it a bit of both?[272] How should we coordinate antitrust cases involving data protection matters with data protection authorities, will there be some sort of institutionalized cooperation, or rather a cooperation on a case-by-case basis? And, how can the case-by-case approach, normally required in dominance investigations, ensure a cohesive data protection policy that addresses industry-wide practices?

In this specific case, FCO stated clearly that monitoring the data processing activities of dominant companies is an essential task of the competition authority, which cannot be fulfilled by a data protection authority[273]. However, in its assessment, the competition authority did take account of the legal principles of data protection laws by noting that "for this purpose, the Bundeskartellamt works closely with data protection authorities."[274] Could this case pave the way to a convergence between competition and data protection rules? Or are we still at a stage where data protection is just a "dimension" of competition law in the tech sector?

The FCO provision seems to go well beyond the boundaries between the traditional jurisdictions of the two agencies, even implying a potential end of privacy law as it has been intended until now. In *Facebook* the FCO went "extra-mile"[275], acting as a self-appointed enforcer of data protection rules and has interpreted data protection rules in a restrictive way that goes far beyond the limits of its legal competence[276]. The theory of harm elaborated by the FCO is grounded on the protection of the constitutional right to informational self-determination. As acknowledged by the same FCO so far, taking into account legal principles to assess abusive practices of a dominant company is possible only under the case-law of the highest German court[277]. On the contrary, according to EU case-law, a breach of the GDPR does not fall within the scope of competition law because it is not as such a harm to competition.

This observation can bring about two conclusions. On the one hand, even where a privacy harm may represent an antitrust harm under Article 102(a), no automatism should follow, unless we want to make antitrust enforcement ancillary to data protection rules. On the other hand, if any law violation is suspected to give a competitive advantage to the infringer (in presence of a harm that competition law can address), then any antitrust authority risks to become a sort of Leviathan[278], intervening for

---

[272] Mareen Ohlhausen, *Privacy and Competition: friends, foes, or frenemies??*, CPI Antitrust Chronicle, February 2019

[273] Bundeskartellamt, "Background information on the Facebook proceeding," published on December 19, 2017, https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Diskussions_Hintergrundpapiere/2017/Hintergrundpapier_Facebook.pdf?__blob=publicationFile&v=6 , question 3, p.2.

[274] Ibid.

[275] G. Buttarelli, supra n.205

[276] the German approach has been endorsed by the European Data Protection Supervisor. See G. Buttarelli, 'Big step towards coherent enforcement in the digital economy', (2019) https://edps.europa.eu/press-publications/press-news/blog/big-step-towards-coherent-enforcement-digitaleconomy_en: "We have consistently supported competition authorities taking action to combat abuse of dominance in a market by means of exploitation of consumers. We are therefore encouraged by this decision by the Bundeskartellamt. This case is the tip of the iceberg - all companies in the digital information ecosystem that rely on tracking, profiling and targeting should be on notice. Take it or leave "privacy policies", opaque and unchallengeable practices like profiling and targeting and multiple obscure third-party agreements for data sharing are, for us, examples of exploitative abuse."

[277] Bundeskartellamt, FAQ's, *supra* , p.6

[278] Colangelo, G. and Maggiolino, M., *Antitrust Über Alles. Whither Competition Law After Facebook?* (March 29, 2019). World Competition Law and Economics Review, 2019, 42(3).

any kind of law infractions (antipollution rules, tax law…). Not by chance, the FCO admitted that the general clause of Section 19(1) GWB is stricter than Article 102(a) TFEU, since it allows prosecuting practices that hardly violate EU competition law[279]. Indeed, the FCO recalled that, according to Article 3(2) of the Modernization Regulation[280], Member States are not precluded from applying on their territory stricter national laws which prohibit or sanction unilateral conduct by undertakings[281].

Even being more optimistic and admitting the possibility of a peaceful coexistence and collaboration between the two authorities, there are other issues to solve, related to the nature and method of the sanctions eventually imposed[282]. A consequence of the *Facebook* investigation may be parallel oversight by both data protection and antitrust authorities. This will raise – also from a legal point of view – questions on how to properly delimit the authorities' jurisdiction.

There may be a case with both data protection and antirust agencies involved, this would imply important changes for the undertakings under investigation. First, fines by data protection may become sort of younger siblings of antitrust ones. Second, if infringements of data protection rules may also qualify as market abuse within the framework of Art. 102 TFEU, would be the undertakings protected from parallel investigations and penalties by the *ne bis in idem* principle[283]?(i.e. a fine decision of one authority prevents the other authority from also imposing a fine.[284])

The ECJ generally shares this approach, but it applies a slightly different standard in competition cases: the principle only applies if the facts and the offender are identical, and the legal interests protected are the same[285]. Therefore, if this latter ECJ's approach is followed, parallel investigations and fines seem plausible. Since the two areas of law serve different legal interests, parallel sanctions by a competition authority and a data protection authority may not violate the *ne bis in idem* principle. However, both fine decisions would still have the infringement of data protection laws as their (sole) substantive basis. German law solves such situations by a "first come first served"[286] general rule which

[279] Bundeskartellamt, Case B6-22/16, *supra*, para. 914

[280] Regulation (EC) 1/2003 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty, (2003) OJ L1/1

[281] Bundeskartellamt, Case B6-22/16, *supra*, para. 914

[282] Stauber P., *Facebook's abuse investigation in Germany and some thoughts on cooperation between Antitrust and Data Protection Authorities*, CPI Antitrust Chronicle, February 2019

[283] Pursuant to the *ne bis in idem* principle, which is enshrined in the German constitution, the Charter of Fundamental Rights of the European Union, and the 7th Protocol to the European Convention of Human Rights, a natural or legal person must not be penalized twice for one and the same cause of action. According to the decision practice of the European Court of Human Rights, the *ne bis in idem* principle prohibits any prosecution resulting from a second offense where that offense is based on identical or substantially similar facts to the ones which were the basis for another offense.

[284] Through the GDPR, entered into force on May 25, 2018, the provisions on financial sanctions for infringements of the GDPR were largely modelled after the respective antitrust rules. Previously, German data protection authorities could only sanction an undertaking with a fine of up to 2 million Euro. Based on the GDPR, the maximum fine now amounts to 20 million Euro. Moreover, undertakings may be sanctioned by a fine of up to 4 percent of worldwide turnover in the last business year. The similarity to the level of antitrust fines under European and German law are manifest: Under European law, the Commission may fine undertakings up to 10 percent of their worldwide turnover. German law provides for the same maximum fine for undertakings, while it also allows for sanctioning individuals with a fine of up to 1 million Euro.

[285] ECJ, judgment of January 7, 2004, joined cases C-204/00 P, C-205/00 P, C-211/00 P, C-213/00 P, C-217/00 P and C-219/00 P para. 338 – *Aalborg Portland et al. /Commission*.

[286] More precisely, the first authority having interviewed the person concerned and, respectively, to whom the police have sent the file after an interview led by the police shall be competent for proceeding with the investigation.

determines the authority competent if the subject matter may be investigated and sanctioned by several authorities.

13.8 An opposite view

Some authors expressed perplexities on why the breach of privacy and data protection would constitute also a breach of antitrust laws[287]. In particular, should antitrust laws hold dominant firms to stricter privacy standards than competing firms without market power? The suspect is that such a practice may distort, rather than protect, competition. According to this perspective, it is difficult to find a good reason for such competition policy intervention. In fact, to impose higher standards and constrains to dominant firms than what are legally required to the other competitors is equivalent to ask by law superior products than rivals. The extreme potential consequence would be a foreclosure of the market, since data-sensitive consumers would find the answer to their need in firms which are already dominant. Moreover, constraining firms in their data-driven activities beyond what is regulated by privacy and data protection laws risk to reduce innovation and to bring inferior services. Empirical evidence even suggests that larger firms generally tend to offer more privacy than small ones[288]. Therefore, it becomes unclear which privacy level would be optimal and which one would be abusive. We lack of a standard hypothetical counterfactual. Here, once again, a difficult trade-off emerges, as requiring dominant firms to collect and to combine less data will typically imply a deterioration of service quality and advertising efficiency, and thereby, a softening of competition. While some consumers may prefer higher privacy standards even if this reduces service quality, other consumers may happily share their data in exchange for better-tailored services.

14. Conclusion

In this last section, we treated in detail two different cases, following a common thread between the two. This thread, namely the competitive importance of personal data and the pressing issue of users' privacy protection online, is a difficult one to deal. Our approach was twofold: on one side, we tried to show which are some operative tools and some applications available to antitrust authorities when it is time to deal with privacy in an antitrust investigation. We exposed the theoretical possibility of considering personal data as a non-monetary price, and to elaborate a theory of harm capable of assessing the direct impact on consumers deriving from a privacy degradation in a service or product. Through this lens, we analysed the Facebook/WhatsApp merger and underlined some aspects which would have been different or improved. On the other side, we presented what is currently the frontier of the antitrust analysis, dealing with the German competition agency's ground-breaking decision. Here, we didn't have any presumption to give a decisive resolution and there are obviously relevant opinions on the issue with an opposite and conflicting view with respect to ours. The literature on the topic is impressive, the scholars and enforcers' level of competence both on the economic and the legal field is impressive, too.

[287] Here we report Haucap J*., 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

[288] Sabatino, L. & G. Sapi (2019), "Online Privacy and Market Structure: An Empirical Analysis," DICE Discussion Paper No. 308, available online at https://ideas.repec.org/p/zbw/dicedp/308.html

For sure, the intersection between competition law and data protection law is an unavoidable issue for all the European and American enforcers and institutions, and it becomes more and more pressing because of the impressive size and market power reached by few data gatekeepers during these last decades. GDPR has been operative for one year, it is proving to be an effective instrument and it is becoming a benchmark in terms of privacy law standards worldwide. The matter is getting more and more in the sights of enforcers and authorities and it will probably be on the agenda for a long time. On the 9th of July 2019, the European Data Protection Supervisor and Federal Commissioner for Data Protection and Freedom of Information of Germany jointly organize the panel discussion on "Data Protection and Competitiveness in the Digital Age" in Brussels[289]. In that occasion, many representatives of different antitrust, data protection and consumer protection authorities debated on the Bundeskartellamt decision. Mr. Giovanni Buttarelli and Mr. Andreas Mundt were present, too.

An opening remark was on to the historical European approach to privacy. The EU data protection framework is solidly based on a culture of privacy protection as an inalienable right aimed at safeguarding personal honour against invasions by private third-parties. These broad rights are enshrined, amongst others, in Articles 7 and 8 of the EU Charter of Fundamental Rights and translated by the General Data Protection Regulation. Then, the main core of the conference was about the prospected interaction between the two kind of authorities involved (one of the recurring jokes pronounced -sometimes with a certain degree of seriousness- is that data protection law has finally become "sexy" and interesting for other enforcers) and on the effectiveness of the current enforcement tools. A reiterated theme was especially a sort of unsatisfaction toward the use of fines, which are no more considered to be enough effective to really "bite" the big tech giants. A clear example is the fine recently imposed by the FTC to Facebook for the Cambridge Analytica case. It is an impressive sanction, namely 5 billion USD, way bigger than the former highest one levied against Google in 2012 (amounting to 22 million USD). The problem is that Facebook had $15 billion in revenue last quarter alone, and $22 billion in profit last year[290].

Therefore, the Bundeskartellamt decision constitutes a novelty also because it carries out an internal divestiture of Facebook's data. It took a stronger and bold resolution. The need for structural remedies capable to correct directly the business game was stressed multiple times during the conference. Currently, agencies have three main instruments to tackle abuses on data collection: (i) to facilitate data portability (Art.20 of GDPR); (ii) to grand access to data, opening the data silos to other rivals on the market; (iii) and to limit the gathering and processing of data, which is the way pursued by the Bundeskartellamt. Another tool debated was interoperability between different services, but this measure face many technical complexities and it is not a viable option at the moment. Mundt stated in more occasions that, since data is the key driver to market dominance, Competition authorities are obliged by law to tackle them. The issues of data access, data portability, interoperability and fostering competition for the market are central also in the latest European commission report[291] wanted by Commissioner Margrethe Vestager. These instruments seem to be the most realistic and viable options in the hands of agencies and regulators. A more radical enforcement – defined by Commissioner

[289] Joint press statement and full video of the conference available at: https://edps.europa.eu/data-protection/our-work/publications/events/data-protection-and-competitiveness-digital-age_en

[290] Nilay Patel, *Facebook's $5 billion FTC fine is an embarrassing joke. Facebook gets away with it again,* The Verge, July 12 2019

[291] European Commission, *Competition Policy for the digital era: Final report*, April 2019

Vestager as the "very last resort"[292] - would be the break-up of Facebook (and more generally of the other big tech giants), as it was recently proposed by some politicians in the US like Sen. Bernie Sanders[293], Sen. Elizabeth Warren and former Vice president Joe Biden.

We conclude the text with some quotations from European Data Supervisor Giovanni Buttarelli's and Commissioner Margrethe Vestager's speeches, resuming some core principles underlying the discussion:

> "All eyes are on Europe and on its leading by example in data protection. In a moment where the whole world is now, finally, acknowledging the importance of high personal data protection standards, and its literally changing legislation and conversations around the GDPR it is imperative that we take the debate a step further. Should we stick to data only, we would run the risk of failing to grasp the bigger picture. […]
>
> Tech titans´ "way of being" reveals a far more complex world where the actual "holy grail" of their brokerage is our *entire existence*. A very small number of giant companies have emerged as effective informational gatekeepers of the content which most people consume. As the protection of personal data is instrumental to the protection of other rights and freedoms, so is the harm to personal data."
>
> […] "Competition law has its historical roots in preserving the democratic assets and outlook of societies. In the EU, it is also a means for the functioning of the internal market. Digital citizens deserve tools which encapsulate a proper response to reality. Competition should go back to its roots and protect those assets and outlook now in danger."[294]

And finally:

> "Businesses will have to be clearer with their users about exactly what they plan to do with their data. […] But that's how it should be. Because data can do great things for us - but we can't buy those benefits at the expense of our values. We can't trade our freedom for better maps, or our democracy for a better social media algorithm. We have a lot to gain from data – but we need to make sure that we use it in a way that is really good for society. […] So we must not be afraid, as a society, to take control of this new world. Because in the end, it's not technology that will decide our future. It's us."[295]

[292] https://www.pymnts.com/news/regulation/2019/eu-antitrust-facebook/
[293] https://www.politico.com/story/2019/05/15/sanders-backs-calls-to-break-up-facebook-1327881
[294] G. Buttarelli, *This is not an article on data protection and competition law*, CPI Antitrust Chronicle, 2019
[295] M. Vestager: *Mackenzie Stuart Lecture,* Cambridge, 4 February 2019

15. Bibliography

Scientific publications

Acquisti, A., L. Brandimarte, and G. Loewenstein (2015), Privacy and human behavior in the age of information. *Science 347*(6221), 509{514

Acquisti, Alessandro and Taylor, Curtis R. and Wagman L. (2016), The Economics of Privacy*, Journal of Economic Literature*, Vol. 52, No. 2, Sloan Foundation Economics Research Paper No. 2580411.

Berthold, S. and R. Böhme (2010), Valuating privacy with option pricing theory, *Economics of information security and privacy*, pp. 187. Springer

Biczók G. and Chia P.H., Interdependent Privacy: Let Me Share Your Data, in David Hutchison and others (eds), *Financial Cryptography and Data Security,* Lecture Notes in Computer Science. Springer Berlin Heidelberg 2013

Botta M. and Wiedemann K., The Interaction of EU Competition, Consumer and Data Protection Law in the Digital Economy. The Regulatory Dilemma in the Facebook Odyssey*, Antitrust Bulletin*

Burnside A. J., 'Setting the Scene', Paper presented at Antitrust, Privacy & Big Data: A Conference Organized in Partnership with Concurrences, 3 February 2015

Buttarelli G., 'Big step towards coherent enforcement in the digital economy', (2019)

Buttarelli G., This is not an article on data protection and competition law, *CPI Antitrust Chronicle*, 2019

Calo R., (2014), Digital Market Manipulation, *82 George Washington Law Review* 995; University of Washington School of Law Research Paper No. 2013-27.

Cate, F. H., (2008), Government Data Mining: The Need for a Legal Framework, *Harvard Civil Rights-Civil Liberties Law Review*, 43

Colangelo, G. and Maggiolino, M., (2019), Antitrust Über Alles. Whither Competition Law After Facebook?, *World Competition Law and Economics Review*, 42(3).

Conti G., Sobiesk E., (2010), Malicious Interface Design: Exploiting the User, 19th International Conference on World Wide Web, ACM, Raleigh

Costa-Cabral F. and Lynskey O., (2017), Family ties: The intersection between data protection and competition in EU law'(54)(1) *Common Market Law Review* 11

CPI Talks with… Terrell McSweeny, *CPI Antitrust Chronicle*, February 2019

Deutscher E., How to measure privacy-related consumer harm in merger analysis? A critical reassessment of the EU Commission's merger control in data-driven markets, *Competition Law for the Digital Economy.* Edward Elgar, ASCOLA Competition Law Series

Dinev T. and Hart P., (2006) An extended privacy calculus model for e-commerce transactions. *Information Systems Research 17* (1), 61-80

Ezrachi A. and Robertson V.H.S.E., (2019), Competition, Market Power and Third-Party Tracking, 42 *World Competition* 5, 8-9

Ezrachi A. and Stucke M.E., *Virtual Competition: The Promise and Perils of the Algorithm Driven Economy*, Harvard University Press, 2016

Farrell J. and Shapiro C., Upward Pricing Pressure and Critical Loss Analysis: Response, *CPI Antitrust Journal,* February 2010

Farrell J., (2012), Can Privacy Be Just Another Good?, *10 J on Telecomm & High Tech L*

Gal M. and Rubinfeld D., (2016), The Hidden Costs of Free Goods: Implications for Antitrust Enforcement, *Antitrust Law Journal* (80) 3, 542

Graef I., (2016), *EU Competition Law, Data Protection and Online Platforms: Data as Essential Facility*, Kluwer Law International

Green P.E. and Rao V.R., (1971), Conjoint Measurement for Quantifying Judgmental Data, 8(3) *Journal of Marketing Research* 355

Green, P.E., Krieger, A.M. and Wind, Y. (2001) Thirty Years of Conjoint Analysis: Reflections and Prospects. *Interfaces*, 31, 56-73

Grunes A.P and Stucke M.E., (2015), No Mistake About It: The Important Role of Antitrust in the Era of Big Data, *University of Tennessee Legal Studies* Research Paper No. 269, 4–6;

Haucap J.*,* 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

Hoofnagle C.J. et al, How Different are Young Adults from Older Adults When it Comes to Information Privacy Attitudes and Policies?, 14 April 2010

Hoofnagle C.J., (2012), Behavioural Advertising: The Offer you can't refuse, 6 *Harv.L.& Pol'y Rev*.273

Hoofnagle C.J., Urban. J., (2014), Alan Westin's Privacy Homo Economicus, 49 *Wake Forest Law Review* 261, UC Berkeley Public Law Research Paper No. 2434800

Hurley S., (2010), The Use of Surveys in Competition and Merger Analysis, 7(1) *Journal of Competition Law & Economics* 45 63

Jensen C. & Potts C., Jensen, C., (2005), Privacy practices of Internet users: Self-reports versus observed behavior. *International Journal of Human-Computer Studies*. 63. 203-227

Johnson E., Bellman S. & Lohse G., (2002) Defaults, Framing and Privacy: Why Opting In-Opting Out. *Marketing Letters*. 13. 5-15.

Kalimo H. and Majcher K.,(2017), The Concept of Fairness: Linking EU Competition and Data Protection Law in the Digital Marketplace, 42 *European Law Review* 210

Kimmel L. and Kestenbaum J., (2014), What's Up with WhatsApp? A Transatlantic View on Privacy and Merger Enforcement in Digital Markets, 29(1) *Antitrust* 48 53

Madden M. and Rainie L., (2015), *Americans' Attitudes About Privacy, Security and Surveillance*, Pew Research Center

Eben, Magali, How Free Internet Services Challenge Traditional Antitrust Tools: Personal Data as a Price, SSRN Electronic Journal, 2016

Magali E., (2018), Market Definition and Free Online Services: The Prospect of Personal Data as Price, I/S: *A Journal of Law and Policy for the Information Society*, Vol.14:2 227

McFadden, Daniel, (1986), The Choice Theory Approach to Market Research, *Marketing Science*, 5, issue 4, p. 275-297

Nazzini R., Privacy and Antitrust: Searching for the (Hopefully Not Yet Lost) Soul of Competition Law in the EU after the German Facebook Decision, *Competition Policy International* (2019)

Newman, J.M. (2015), "Antitrust in Zero-Price Markets: Foundations", *University of Pennsylvania Law Review*, 164, 149-206.

Ocello E., Sjödin C., and Subočs A., 'What's Up with Merger Control in the Digital Sector? Lessons from the Facebook/WhatsApp EU Merger Case', 1 *Competition Merger Brief* (February 2015)

Ohlhausen M. and Okuliar A., (2015), Competition, consumer protection, and the right (approach) to privacy, 80(1) *Antitrust Law Journal* 121-151 ff

Ohlhausen M., Privacy and Competition: friends, foes, or frenemies??, *CPI Antitrust Chronicle*, February 2019

Pasquale F., (2013), Paradoxes of Digital Antitrust: Why the FTC Failed to Explain its Inaction on Search Bias, *Harvard Journal of Law & Technology* - Occasional Paper Series 1, 7

Pasquale F.A. (2013), "Privacy, Antitrust and Power", *Georges Mason Law Review* 20(4), 1009-1024;

Pu Y. and Grossklags J., (2015), Using Conjoint Analysis to Investigate the Value of Interdependent Privacy in Social App Adoption Scenarios, Research Paper presented at the 36th International Conference on Information Systems, Fort Worth 2015, 2

Purcell K., Brenner J., and Rainie L., (2012) *Search Engine Use 2012*, Pew Research Center

Rao A., Schaub F., Sadeh N., (2014), What do they know about me? Contents and Concerns of Online Behavioral Profiles, Sixth ASE International Conference Privacy, Security, Risk and Trust (PASSAT'14), Cambridge

Sabatino, L. & Sapi G., (2019), Online Privacy and Market Structure: An Empirical Analysis, *DICE Discussion* Paper No. 308, (2019)

Schepp, Wambach, (2016), On Big Data and Its Relevance for Market Power Assessment, *Journal of European Competition Law & Practice*, 7, 2

Slovic P., (1995), The Construction of Preference, *American Psychologist*. 50. 364-371.

Stauber P., Facebook's abuse investigation in Germany and some thoughts on cooperation between Antitrust and Data Protection Authorities, *CPI Antitrust Chronicle*, February 2019

Stucke M. E., (2013), Is Competition Always Good?, 1 *Journal of Antitrust Enforcement*

Stucke M.E. & Grunes A.P., (2016), *Big Data and Competition Policy*, Oxford University Press

Stucke M.E., 'Behavioral Exploitation and its Implications on Competition and Consumer Protection Policies', in Swedish Competition Authority (ed), *The Pros and Cons of Consumer Protection* (Stockholm: Konkurrensverket Swedish Competition Authority 2012), pp 77–122.

Stucke, M.E. and Ezrachi A., (2015), When Competition Fails to Optimise Quality: A Look at Search Engines, *University of Tennessee Legal Studies* Research Paper No. 268, 36

Swarmy K., 'Analyzing Tesco—The Analytics Behind a Top-Notch Loyalty Programme', *Big Data Analytics*, 21 August 2011

Sweeney L., (2000), *Simple Demographics Often Identify People Uniquely,* Carnegie Mellon University, Data Privacy Working Paper 3, Pittsburgh

Tsai, J. Y. et al., (2011), The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study, *Information Systems Research*, vol. 22, no. 2, pp. 254–268.

Turow J., Hennessy M. and Draper N., (2015), *The Trade-off Fallacy: How Marketers Are Misrepresenting American Consumers and Opening Them Up to Exploitation*, University of Pennsylvania Annenberg School of Communication

Waehrer, Keith. (2015), Online Services and the Analysis of Competitive Merger Effects in Privacy Protections and Other Quality Dimensions, *SSRN Electronic Journal*. 10.2139/ssrn.2701927.

White, T. B., et al., (2008), Getting Too Personal: Reactance to Highly Personalized Email Solicitations, *Marketing Letters*, vol. 19, no. 1, pp. 39–50.

Other publications and reports

Article 29 Working Party, (April 2014), *Opinion 05/2014 on Anonymisation Techniques*, WP 216

Autorité de la concurrence and Bundeskartellamt, (2016), *Competition law and data*

Belgian Competition Authority, Beslissing BMA-2015-P/K-27-AUD van 22 september 2015, Zaken nr. MEDE-P/K- 13/0012 en CONC-P/K-13/0013, *Stanleybet Belgium NV/Stanley International Betting Ltd en Sagevas S.A./World Football Association S.P.R.L./Samenwerkende Nevenmaatschappij Belgische PMU S.C.R.L. t. Nationale Loterij NV*, par.44-48.

Boston Consulting Group, (2012), *The Value of our Digital Identity*

Bundeskartellamt, *Decision B6-22/16*, 11th July 2019

Cisco, (2014), *Cisco Global Cloud Index: Forecast and Methodology, 2013–2018.*

CNIL, (2014) *The CNIL's Sanctions Committee Issues a 150 000 € Monetary Penalty to Google Inc.*

Commission Decision of 11 March 2008, Case M.4731 *Google/ DoubleClick*

Commission Decision of 18 February 2010, Case M. 5727 *Microsoft/Yahoo! Search Business*

Commission Decision of 3 October 2014, Case M.7217 *Facebook/WhatsApp*

Commission Decision of 6 December 2016, Case M. 8124 *Microsoft/LinkedIn*.

Commission Decision of 7 October 2011, Case M.6281 *Microsoft/Skype*

Commission Staff Working Document (2017) on the free flow of data and emerging issues of the European data economy, SWD 2

Competition and Markets Authority, (2015), *The Commercial Use of Consumer Data: Report on the CMA's Call for Information*

De Streel A., Bourreau M., Graef I., Big Data and Competition Policy: Market power, personalised pricing and advertising, *CERRE*, 2017

Electronic Frontier Foundation, (2015), *Who Has Your Back? Fifth Annual Report on Online Service Providers' Privacy and Transparency Practices Regarding Government Access to User Data*

Electronic Privacy Information Center, (2014), *In Re WhatsApp*, 2014

European Commission, (2018a), *Consumer market study on online market segmentation through personalised pricing/offers in the European Union final report*

European Commission, (2019), *Competition Policy for the digital era: Final report*

European Commission, (2018b), *Guidelines on the Assessment of Non-Horizontal Mergers under the Council Regulation on the Control of Concentrations Between Undertakings*

European Commission, (2015), *Why We Need a Digital Single Market* (2015)

European Data Protection Supervisor (EDPS), (2014), *Privacy and Competitiveness in the Age of Big Data: The Interplay Between Data Protection, Competition Law and Consumer Protection in the Digital Economy, Preliminary Opinion*

European Data Protection Supervisor, (2015), *Towards a New Digital Ethics: Data, Dignity and Technology, Opinion 4/2015*

Federal Trade Commission, (2014), *Data Brokers: A Call for Transparency and Accountability*

IDC, (2016), *Europe's Data Marketplaces – Current Status and Future Perspectives, Report for the European Commission*

Monopolkommission, (2015), *Competition policy: The challenge of digital markets*, Special Report 68

OECD (2013), Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value, *OECD Digital Economy Papers*, No. 220, OECD Publishing.

OECD, (2014), *Data-Driven Innovation for Growth and Well-Being: Interim Synthesis Report*

OECD, (2009), *Policy Roundtables: Two-Sided Markets*

OECD, (2013), *The Role and Measurement of Quality in Competition Analysis*

Office of Fair Trading (OFT), (2013), *ME/6167/13: Completed Acquisition by Motorola Mobility Holding (Google, Inc.) of Waze Mobile Limited*

The Executive Office of the President, (2014), *Big Data: Seizing Opportunities, Preserving Values* ('White House Big Data Report').

US Department of Justice (DOJ) and Federal Trade Commission (FTC), (2010), *Horizontal Merger Guidelines*

Press articles and Press releases

Auction.com, (2014), *Auction.com Launches Real Estate's First Nowcast—Leverages Industry, Transactional and Google Search Data to Provide Accurate Real-Time Market Intelligence*, Press Release

Autorité de la concurrence, (2014), *Décision 14-MC-02 du 9 septembre 2014 relative à une demande de mesures conservatoires présentée par la société Direct Energie dans les secteurs du gaz et de l'électricité*

Bundeskartellamt, *Facebook*, Press release, 7th February 2019

Bundeskartellamt, *Facebook*, FAQ's, 7th February 2019

Competition Commissioner Vestager, Competition in a big data world, DLD 16 Munich, Speech 17 January 2016.

Datatilsynet, (2015), *The Great Data race: How commercial utilisation of personal data challenges privacy*. Report

Döpfner M., An Open Letter to Eric Schmidt: Why We Fear Google, *Frankfurter Allgemeine*, 17 April 2014

Drozdiak N., WhatsApp to Drop Subscription Fee, *Wall Street Journal*, 18 January 2016

Duhigg C., How Companies Learn Your Secrets, *NY Times*, 16 February 2012

European Commission, 'Fact Sheet: Commission Sends Statement of Objections to Google on Comparison Shopping Service', 15 April 2015

European Commission, 'Mergers: Commission Approves Acquisition of WhatsApp by Facebook', Press Release, 3 October 2014

European Commission, 'Press Release - Commission alleges Facebook provided misleading information about WhatsApp takeover', 20 December 2016

Federal Trade Commission, 'FTC Approves Final Order in Case About Google Billing for Kids' In-App Charges Without Parental Consent', Press Release, 5 December 2014

Federal Trade Commission, 'FTC Charges Deceptive Privacy Practices in Google's Rollout of Its Buzz Social Network: Google Agrees to Implement Comprehensive Privacy Program to Protect Consumer Data', Press Release, 30 March 2011

Federal Trade Commission, 'Google Will Pay $22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser', Press Release, 9 August 2012

Geradin and Kuschewsky (n 9), 37; European Commission, 'Commission probes allegations of antitrust violations by Google - Press Relase of 30 November 2013 - IP/10/1624'

Goel V., 'Flipping the Switches on Facebook's Privacy Controls', *New York Times*,29 January 2014

Greenberg A., 'Rating Tech Giants on Privacy: Google Slips, WhatsApp Fails', *Wired*, 18 June 2015

Harbour P.J., 'Dissenting Statement of Commissioner Pamela Jones Harbour in the Matter of Google/DoubleClick F.T.C. File No. 071-0170' (n 9)

Howarth B., 'How Tesco's loyalty card transformed customer data tracking', *CMO*, 21 May 2015

Kang C., *F.T.C. Approves Facebook Fine of About $5 Billion,* The New York Times, 12 July 2019.

Letter from the Article 29 Data Protection Working Party to Larry Page, 16 October 2012

Letter from Jessica Rich, Director, Bureau of Consumer Protection to Erin Egan, Chief Privacy Officer, Facebook, Inc and Anne Hoge, General Counsel, WhatsApp Inc, 10 April 2014 ('Rich Letter')

Mims C., Ask M for Help: Facebook Tests New Digital Assistant: Single Interface Could Replace Web Searches and Apps on Mobile Devices, *Wall Street Journal*, 9 November 2015

Moerel L., inaugural address Tilburg Law School, 'Big Data Protection: How to Make the Draft EU Regulation on Data Protection Future Proof', 14.02.2014.

Newton C., Google Reaches $7 Million Settlement with States over Street View Case, *CNET*, 12 March 2013

Patel N., Facebook's $5 billion FTC fine is an embarrassing joke. Facebook gets away with it again*, The Verge*, July 12 2019

Public Citizen, *Mission Creep-y: Google Is Quietly Becoming One of the Nation's Most Powerful Political Forces While Expanding Its Information-Collection Empire*, November 2014

Schmidt E., Executive Chairman of Google, 'The New Gründergeist', *Google Europe Blog*, Posted: 13 October 2014

Schmidt E., Executive Chairman of Google, Why Google Works, *Huffington Post*,20 January 2015

Seetharaman D., Facebook Prods Users to Share a Bit More: Amount of New Content Posted Has Slipped, Leading Social Network to Try to Prompt Conversation, *Wall Street Journal*,2 November 2015

Speech by M. Vestager - European Commissioner for Competition, 'Setting innovation free'. Bpifrance Inno Génération: Paris 2017

Speech by Vice Commissioner Reding, 'Personal data is the currency of today's digital market;' The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age – Innovation Conference Digital, Life, Design', Munich, 22 January 2012

Speech by Vice-President Almunia, 'Competition and personal data protection', 26 November 2012

Speech by Vice-President Kroes, 'Big Data for Europe', 7.11.2013

Steel E., Financial worth of personal data comes in under a penny a piece, *Financial Times*, 12 June 2013.

Tanner A., (2013), Never Give Stores your zip code. Here's why, *Forbes*

Tech2 News, WhatsApp Security Flaw Allows Anyone to Track You Regardless of Your Privacy Settings, 13 February 2015

The Economist, "Getting to know you", September 2014.

Troy M., ‘What’s Worse than Your Mom Seeing Your Web History? The NSA, *Google’ Survata Blog*, 27 October 2014

Vestager M., ‘Mackenzie Stuart Lecture’*,* Cambridge, 4 February 2019

Wolfie C., “Corporate surveillance in everyday life: How companies collect, combine, analyse, trade, and use personal data on billions”, *Cracked Labs*, 2017