COLLEGE OF EUROPE
NATOLIN (WARSAW) CAMPUS
EUROPEAN INTERDISCIPLINARY STUDIES

Privacy, Pricing and Big Data – An Interdisciplinary Review of the Impact of the General Data Protection Regulation on Online Price Discrimination

Supervisor: Mario Mariniello

Thesis presented by
Yannic Blaschke
for the Degree of Master of Arts in European Interdisciplinary Studies

Academic Year 2017 - 2018

Statutory Declaration

I hereby declare that this thesis has been written by myself without any external unauthorised help, that it has been neither submitted to any institution for evaluation nor previously published in its entirety or in parts. Any parts, words or ideas, of the thesis, however limited, and including tables, graphs, maps etc., which are quoted from or based on other sources, have been acknowledged as such without exception.

Moreover, I have also taken note and accepted the College rules with regard to plagiarism (Section 4.3 of the College study regulations).

_____

Yannic Blaschke

Déclaration sur l'honneur

Je déclare sur l'honneur que ce mémoire a été écrit de ma main, sans aide extérieure non autorisée, qu'il n'a été déposé auparavant dans aucune autre institution pour évaluation, et qu'il n'a jamais été publié, dans sa totalité ou en partie. Toutes parties, mots ou idées, aussi limités soient-ils, y compris des tableaux, graphiques, cartes etc. qui sont empruntés ou qui font référence à d'autres sources bibliographiques sont présentés comme tels, sans exception aucune.

Je déclare également avoir pris note et accepté les règles relatives au plagiat (section 4.3 du règlement d'études du Collège).

_____

Yannic Blaschke

Abstract

Through continuous developments in computing power and profiling algorithm technology, the possibilities for online suppliers to target their price offers in accordance with consumers' willingness to pay have vastly increased. With the entry into force of the General Data Protection Regulation of the European Union, however, the processing of the personal data that is vital for the personalisation of online services becomes subject to a number of strict legal provisions. This thesis assesses the respective effects that the regulation will have on online price discrimination practices through an interdisciplinary approach. The GDPR's material scope and the rights it confers to individuals are interpreted in the light of economic theory on privacy and price discrimination and are cross-matched with insights from computer science to derive inferences on the implementation of the legislation in the context of big data analytics. Integrating the findings of this analysis under consideration of the case of the geographic price-personalisation company Darwin Pricing, the study concludes that the regulation will influence online price discrimination in three ways: A direct impact on its technical implementation, a behavioural empowerment impact on its technical implementation and a behavioural empowerment impact on societal welfare. In addition to an analysis of the practical implications of each type of impact, the thesis points out several of the legal, technical and ethical questions regarding online price discrimination that are left open under the new regulatory privacy framework and gives indications for further research.

Key Words

General Data Protection Regulation
Price Discrimination
Big Data
Artificial Intelligence
Consumer Targeting

Abbreviations

AI	Artificial Intelligence
ENISA	European Union Agency for Network and Information Security
EU	European Union
CJEU	Court of Justice of the European Union
GDPR	General Data Protection Legislation
IP-Address	Internet Protocol Address
PET	Privacy Enhancing Technologies

CONTENTS

1. Introduction

On the 27th of April, the European Union (EU) adopted the General Data Protection Regulation (GDPR), an update of its 1995 Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data that will bring significant changes to the way personal data processing companies can exercise their business. The regulation, which applies uniformly in all Member States of the Union from the 25th of May 2018 onwards, has been widely considered as a substantial enhancement of the previous EU legal framework that reacts to a growing awareness of citizens on how their personal data is used, especially in an online environment.[1] The Commission argues that the legislation will increase consumer trust, facilitate international data flows and encourage innovation, and thus regards the transition to a single EU wide privacy framework as a major step towards its envisioned Digital Single Market.[2] Meanwhile, representatives of major stakeholders such as the e-commerce business have acknowledged the GDPR to be among the "milestones towards increasing consumer trust in the digital economy by strengthening privacy rights and data protection rights".[3] Indeed, the Regulation considerably increases the scope of what is regarded as personal data by including online identifiers such as IP addresses or Cookies[4] and provides citizens with a substantial increase in control about the processing of their personal data, giving them for instance an enhanced 'right to be forgotten' and requiring the processing companies to ask for the data subjects' unambiguous consent to do so.[5] As highlighted by the plethora of guidelines, recommendations and reports that are currently being published concerning the implementation of the GDPR in data processing businesses, the adaptation of the new privacy regime poses an enormous challenge for the

[1] Lawrence Ryz and Lauren Grest, 'A new era in data protection', in: *Computer Fraud & Security*, Vol.2016, No.3, 2016, p.18.
[2] European Commission, *EU Data Protection Reform: better rules for European businesses.* Available at: https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-business_en.pdf (consulted on , p. 2-3.
[3] Ecommerce Europe, *The General Data Protection Regulation is now a reality!*, 2018. Available at: https://www.ecommerce-europe.eu/news-item/the-general-data-protection-regulation-is-now-a-reality/ (consulted on 6.2.2018).
[4] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, Art. 4 (1).
[5] *Ibid.*, Art. 17, 7.

emerging digital economy, not only within the EU but in principle everywhere where the personal data of EU citizens are processed.[6]

The ongoing adaptation process, in turn, raises interesting questions on the compatibility of key practices of personal data-driven businesses with the EU's envisioned standard of privacy, especially in regard to providing consumers with personalised offers online. One of the most interesting tools that might be affected by the GDPR in this regard is companies' ability to price discriminate, meaning a situation in which "two or more similar goods are sold at prices that are in different ratios to marginal costs".[7] While the basic economic concept of price discrimination is not a new one, the rise of information technology in the past two decades has enabled an unprecedented advance in terms of the amount of data that companies can obtain about their customers, leading to a capacity of placing offers in a more personalised way than ever before.[8] Indeed, such digital personalisation based on consumer tracking technologies has not only found its introduction into the realm of marketing and advertising but has also been proven to be an applied instrument for a number of online vendors and travel websites.[9] Privacy regulation seems to have, in turn, a mitigating influence on the effectiveness of the technologies that enable such consumer targeting. Researchers noted, for instance, an average 65% decrease in effectiveness of personalised advertising as a result of the legal framework posed by the EU's 1995 data protection directive.[10] Since online price discrimination is directly dependent on the collection and processing of user data and is thus likely to be similarly affected by the new provisions of the GDPR, it is thus reasonable to assess the potential consequences that are likely to arise after the Regulation's entry into force in May 2018 in terms of online price discrimination. Doing so, this study will build on the work of scholars who have analysed the general applicability of the regulation's provisions to online price discrimination[11] and will

[6] Consider, for instance, the Commission's website on GDPR implementation or Microsoft's in-depth adaptation guide: European Commission, *Data Protection - better rules for small business.* Available at: http://ec.europa.eu/justice/smedataprotect/index_en.htm (consulted on 6.2.2018).
Microsoft France, *GDPR - Get Organized and Implement the Right Processes for Compliance with the GDPR*, Issy-Les-Moulineaux, 2017, pp.1-69.
[7] George J. Stigler, *The theory of price*. Macmillan, New York, 1987, 371 p.
[8] Xia Zhao and Ling Xue, 'Competitive Target Advertising and Consumer Data Sharing', in: *Journal of Management Information Systems*, Vol.29, No.3, 2012, p.189-190.
[9] For an example from the United States, see Aniko Hannak, Gary Soeller, David Lazer, Alan Mislove and Christo Wilson, 'Measuring Price Discrimination and Steering on E-commerce Web Sites', in: *Proceedings of the 2014 Conference on Internet Measurement Conference*, Vancouver, BC, Canada, 2014, p. 13.
[10] Avi Goldfarb and Catherine E. Tucker, 'Privacy Regulation and Online Advertising', in: *Management Science*, Vol.57, No.1, 2011, p.68.
[11] The most noteworthy works in this regard are the ones of Frederik Zuiderveen Borgesius and Joost Poort, 'Online Price Discrimination and EU Data Privacy Law', in: *Journal of Consumer Policy*, Vol.40, No.3,

broaden the scope of analysis through an interdisciplinary review of the potential effects of the legislation, both regarding the technical implementation of online price discrimination and potential welfare implications.

2017, pp. 347-366 and Richard Steppe, 'Online price discrimination and personal data: A General Data Protection Regulation perspective', in: *Computer Law & Security Review*, Vol.33, No.6, 2017, pp. 768-785.

2. Methodology

To analyse the topic outlined above, this study will follow the following research question:

RQ: In what way will the General Data Protection Regulation impact on online price discrimination?

Understanding and evaluating this type of exploratory research question requires an interdisciplinary research approach: The General Data Protection Regulation is (i) a legal document that regulates (ii) innovative technologies with (iii) a possible indirect economic effect on price discrimination. The research problem thus qualifies as an interdisciplinary one; insights from economics are needed for its understanding just as well as methods of legal interpretation and evaluations derived from computer science; each of the involved disciplines addressing a valid part of the identified problem.[12]

To gather the relevant insights from the economic and computer science disciplines, two full-scale literature researches are conducted on each field.[13] For the first one, the guiding sub-question will be:

SQ1: To what extent is the concept of price discrimination applicable to the world wide web environment?

The corresponding Chapter 3 will thus comprise a literature review of the standard scholarship on the economic concept of price discrimination as well as the outlining of existing literature that has hitherto matched this concept with the world wide web environment. The second full-scale literature research will address the issue of behavioural targeting from a technical perspective, asking the sub-question:

SQ2: What are the current technologies available for online price discrimination?

Chapter 4 will thus focus on the identification of the key technologies for online price discrimination by providing the necessary definitions and analysing the applicable insights from computer science.

After having conducted the literature researches, the gathered insights will be synthesised and matched with the legal provisions of the GDPR in Chapter 5. The aim is ultimately to provide an interdisciplinary integration by "critically evaluating disciplinary

[12] For a further definition and conceptualisation of interdisciplinary research, see Allen Repko and Rick Szostak, *Interdisciplinary Research: Process and Theory* (3rd edition). Sage, Los Angeles, 2017,
[13] *Ibid.*, p. 138.

insights and creating common ground among them to construct a more comprehensive understanding".[14] Conducted in an exploratory setting where many of the involved factors remain opaque and some variables (such as consumer behaviour) will only be possible to be empirically observed after the entry into force of the GDPR, it must be clear from the outset that the study does not attempt to give absolute answers. The aim is much more to conceptualise the impact of the regulation in a multidimensional way that allows for an anticipation of the most likely effects and the identification of issues for further research.

To inform the research process nevertheless with some empirical insights, the theoretical considerations are accompanied by a case study of the price-personalising company Darwin Pricing. While a behavioural study on consumer preferences under their new rights conferred by the GDPR would be another highly valuable source of empirical insight, such an approach is more difficult to implement prior to the entry into force of the regulation. The choice of an enterprise as a unit of analysis is, in turn, considered beneficial here because personal data processing business owners will have to comply with the regulation from the 25th of May onwards and are thus likely to have implemented respective requirements already at the point of inquiry. Naturally, the problem that arises regarding generalisation when insights are inferred from a single case should be noted and taken with utmost seriousness.15 However, in the exploratory setting of this study, the chosen common case16 does not fulfil the purpose of a full-fledged generalisation of the acquired information to the general population of price-personalising companies, but to obtain a better understanding of the concepts and problem areas developed in the analysis section and to identify issues for further empirical research.

[14] *Ibid.*, p. 221.
[15] Robert K. Yin, *Case Study Research - Design and Methods* (5th edition). SAGE Publications, Thousand Oaks, 2014, pp. 20-21.
[16] Cf. *Ibid.*, p. 52.

3. Economic Theory and Literature Review

This chapter will develop a theoretical framework for the assessment of online price discrimination by outlining the main concepts of price discrimination literature and presenting the existing literature on price discrimination and privacy in online environments.

3.1. Economic Theory on Price Discrimination and Privacy

A classic definition of differential pricing is that "price discrimination is present when two or more similar goods are sold at prices that are in different ratios to marginal costs", which is beneficial because it does not include differences in prices that occur for non-discriminatory reasons such as transport costs to different geographical areas.[17] It is traditionally argued that a firm must fulfil three conditions to be able to price-discriminate, scilicet (i) having some market power, (ii) having the ability to sort customers and (iii) being able to prevent resales.[18] Under the assumptions of monopolistic competition and an absence of resales, we can distinguish between three types of price discrimination in economic theory: First-, second- and third-degree price discrimination.[19] First degree or 'perfect' price discrimination occurs when a monopolistic seller is able to charge each customer a price that is based on the individuals willingness to pay, which maximises producer and eliminates consumer surplus through the gradual adjustment of charged prices down to the firms marginal cost level.[20] In a situation where consumers buy multiple units of a product, the firm would adjust its prices for each of the units sold. In regard to efficiency, there is no difference between the quantity of output in perfect competition and perfect price discrimination with a monopolist seller, but the output is significantly higher than in a situation with a monopolistic seller and uniform pricing. As a result of the monopolist's increased supply rate, the overall creation of welfare is of less concern in this case then the distribution of welfare between consumers and suppliers. In comparison, second-degree price discrimination or non-linear pricing describes the practice of charging different prices not based on individual characteristics of the customer, but on the quantity purchased.[21] More sophisticated models of second degree price discrimination entail two-part tariffs, through which a company charges a lump sum

[17] Hal R. Varian, 'Chapter 10: Price discrimination', in: R. Schmalensee and R. Willing (ed.), *Handbook of Industrial Organization* (1st). Elsevier, Amsterdam, 1989, p.598. The definition is originally provided by Stigler, *op cit.*, pp. 371.
[18] Varian, *op cit.*, p.599.
[19] Dennis W. Carlton and Jeffrey M. Perloff, *Modern Industrial Organization* (4th edition). Addison-Wesley, Boston, 2005, p.280.
[20] *Ibid.*, pp.280-283.
[21] *Ibid.*, p.298.

fee for the right to purchase a certain good as well as a usage fee per unit, and tie in sales that bind the right to purchase one good at a certain price to the obligation of buying another one as well. [22] Second-Degree price discrimination does thus not require information about the customer's specifications because it is the customer him-/herself who chooses the quantity based pricing model. Finally, third-degree price discrimination occurs when a company charges different unit prices to different groups of customers. This represents a case of imperfect price discrimination that can be exercised through geographical, but also opportunity cost driven segmentation of customers, the latter occurring for example when customers are charged different prices based on their willingness to wait to consume a product.[23]

Although their relevance crucially depends on factors such as the price elasticity of certain goods and services or the ability of customers to switch between the sections of a segmented market (demand linkage), some general advantages and disadvantages for companies and customers can generally be asserted to price discrimination practices. For instance, a firm that is able to price discriminate might also be able to expand into new markets that would be unprofitable under uniform pricing, leading to a pareto welfare gain.[24] Taking into consideration consumption externalities, the assumption of welfare gains through price-discrimination induced opening of new markets has been challenged, but the general analysis that overall welfare in third-degree price discrimination can be positive holds even in the presence of such externalities.[25] Segmenting markets can also enhance welfare by letting companies enjoy greater economies of scale: Being able to charge a lower price in a less profitable market can result in an increase in output quantity of a firm, thus decreasing the output price per unit when economies of scale are present.[26] Companies might also be able to use their infrastructures more efficiently, which applies especially to firms with high fixed costs: In a case where an additional customer increases marginal cost only to a very limited extent, the additional revenue can either add to the

[22] *Ibid..*, p.298-302.
[23] *Ibid.,*. p.288.
[24] Stephen K. Layson, 'Market-Opening under Third Degree Price Discrimination', in: *Journal of Industrial Economics*, Vol.42, No.3, 1994, p.339.
[25] Tomohisa Okada and Takanori Adachi, 'Third-Degree Price Discrimination, Consumption Externalities, and Market Opening', in: *Journal of Industry, Competition and Trade*, Vol.13, No.2, 2013, p.216., Takeshi Ikeda and Tatsuhiko Nariu, 'Third-Degree Price Discrimination in the Presence of Asymmetric Consumption Externalities', in: *Journal of Industry, Competition and Trade*, Vol.9, No.3, 2009, pp.260-261.
[26] Park Donghyun, 'Price Discrimination, Economies of Scale, and Profits', in: *Journal of Economic Education*, Vol.31, No.1, 2000, p.74.

achieved profits or to the mere covering of the fixed costs.[27] There are also arguments that firms can use price discrimination for achieving a more efficient inventory management, even in the presence of demand leakage. The market segmentation a firm carries out by charging differentiated prices to different groups of customers does in this way not only serve the purpose of profit maximisation, but also to efficiently manage its stocks and product orders.[28]

As evident from the remarks outlined above, price discrimination depends crucially on the amount of information a company has available about its customers. Although there are of course countless ways through which companies can segment markets by using non-personal data, it can be stated that the informational privacy of customers, defined as their ability to choose between the protection and sharing of their personal data based on the respective trade-offs[29] is generally detrimental to a company's ability to price-discriminate if consumers decide not to share their data. From the consumers perspective, the revealing of information in an environment they know to be price-discriminatory can be either advantageous or disadvantageous for them, depending on whether the disclosure of their data will result in a higher or in a lower price charged.[30]

[27] Economics Online, *Price discrimination as a profit maximising strategy*. Available at: http://economicsonline.co.uk/Business_economics/Price_discrimination.html (consulted on 2018/02/18/).
[28] Syed Asif Raza, 'An integrated approach to price differentiation and inventory decisions with demand leakage', in: *International Journal of Production Economics*, Vol.164, 2015, p.106.
[29] Alessandro Acquisti, Curtis R. Taylor and Liad Wagman, 'The Economics of Privacy', in: *Journal of Economic Literature*, Vol.52, No.2, 2016, p.2.
[30] Hal R. Varian, 'Economic Aspects of Personal Privacy', in: W. H. Lehr and L. M. Pupillo (ed.), *Internet Policy and Economics* (2nd). 2009, pp.103-104.

3.2. Price Discrimination and Privacy in Online Environments

As mentioned before, the proliferation of information technologies and the rise of the Web 2.0[31] has produced a shift from a situation in which internet users were mere consumers of online services to a digital economy in which users have become producers of highly sensitive data that enables an analysis of their actions, interests and intentions on an unprecedented scale.[32] The availability and analysis of such data has given rise to the concept of online behavioural targeting, a practice in which companies create individualised profiles of customers by monitoring the online activities of customers and subsequently present them with highly personalised offers.[33] While the vast majority of current literature on behavioural targeting addresses the issue of online advertising, scholars have also started to express interest in the question on how the proliferation of such technologies might influence the pricing decisions of companies that offer goods and services online.

In general, it can be held that there exist two opposing developments regarding the enterprise-customer relationship in online environments. On the one hand, the targeting technologies offer companies the potential of charging customers prices based on their estimated willingness to pay, which could be seen as an approximation towards a situation of first-degree price discrimination.[34] On the other hand, customers have also been empowered by the online environment, which allows them to do extensive price-comparisons between companies to choose the best offers. While predictions that online competition would drive prices of goods and services to the marginal cost level have not realised, the instant price-comparison customers can conduct via search engines or price comparison sites does certainly provide a powerful tool of enhancing the level of information asymmetry on the consumer side.[35] The arbitrage process of using such search mechanisms does however constitute a "double-edged sword" because it produces a high amount of customer-specific data itself, which can in turn again be used for

[31] Web 2.0 commonly refers to the development of the internet as a platform that enables users to participate in the generation of content, for example through wikis or social media. Cf. Tim O'reilly, *What Is Web 2.0*. 2018, Available at: http://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html?page=1 (consulted on 15.2.2018).
[32] Acquisti, Taylor and Wagman, *op cit.*, p.3.
[33] Robert J. Aalberts, Alexander Nill and Percy S. Poon, 'Online Behavioral Targeting: What Does the Law Say?', in: *Journal of Current Issues & Research in Advertising*, Vol.37, No.2, 2016, p.96.
[34] For an in-depth literature review on first-degree price discrimination in online environments, see Silvia Merler, *Big data and first-degree price discrimination.* Bruegel, 2017, Available at: http://bruegel.org/2017/02/big-data-and-first-degree-price-discrimination (consulted on 21.2.2018).
[35] Michael R. Baye, J. Rupert J. Gatti, Paul Kattuman and John Morgan, 'A Dashboard for Online Pricing', in: *California Management Review*, Vol.50, No.1, 2007, p.203.

targeting purposes.[36] The result of the diverging trends in customer targeting and customer arbitrage can be characterised as a situation in which the "level of sophistication" of customers crucially matters: Whereas "naïve" customers will not question prices offered to them and will thus allow companies to extract their surplus, "sophisticated customers" who are aware of the presence of tracking can use their knowledge to circumvent the online pricing tools or even manipulate their data entries to receive a more beneficial offer, reducing the surplus of the firm.[37] In this situation, scholars have concluded that the added value of privacy enforcing regulation ultimately depends on the level of customer sophistication, because the adoption of personalising technologies is in the end only profitable to companies if customers either have no circumvention methods at their disposal or do not make use of such methods on a larger scale.[38] However, the criteria outlined for industries that can benefit the most from preferential pricing arguably suit the online environment very well: it is computer-mediated and therefore allows for the collection and storage of customer information, and where services are provided fixed costs are often rather low (e.g. software, video on demand etc).[39] It is also evident that although the achievement of anonymous purchases through the use of anti-tracking software is not per se difficult or costly, customers still do not seem to implement them on a large scale: While according to Eurostat, about 53% of EU citizens are aware that online cookies[40] can be used to trace their movements of the internet, only 28% have ever changed their cookie settings to limit such tracking.[41] This may underline the problem for consumers that lies in the opaque nature of privacy in online environments, where trade-offs such as whether a protection from price discrimination may be worth the potential disadvantage of not receiving advertisements and targeted offers are often hard to assess.[42] Privacy decisions of individuals are often led by misguided perceptions of the costs and benefits of such trade-offs as well as social and cultural norms; they are therefore often highly context-dependent and thus inconsistent even for consumers with a high privacy sensitivity.[43] In the light of such behavioural factors, the low salience of

[36] *Ibid.*
[37] C. R. Taylor, 'Consumer privacy and the market for customer information', in: *The RAND Journal of Economics*, Vol.35, No.4, 2004, p.643.
[38] *Ibid.*, also see the conclusions of Alessandro Acquisti and Hal R. Varian, 'Conditioning Prices on Purchase History.', in: *Marketing Science*, Vol.24, No.3, 2005, p.33.
[39] Acquisti and Varian, *op cit.*, pp.33-34.
[40] See definition provided below.
[41] Eurostat, *Privacy and protection of personal information* , Available at: http://appsso.eurostat.ec.europa.eu/nui/submitViewTableAction.do (consulted on 22.2.2018).
[42] Alessandro Acquisti, Laura Brandimarte and George Loewenstein, 'Privacy and human behavior in the age of information', in: *Science*, Vol.347, No.6221, 2015, pp.509-510.
[43] *Ibid.*, pp.510-512.

data protection issues and the widespread lack of adopted counter-measures, it is fair to assume that behavioural targeting practices are generally attractive from the supply side of view.

However, some disincentives to apply price discrimination even in a situation where overall customer sophistication is low can still be identified. Firstly, price discrimination is heavily disliked by consumers in general. It has been stated that this strong discontent could be potentially explained with the behavioural economics concept of loss or regret aversion, which states that people tend to object to situations in which an action they could (not) have taken would have led to a better outcome, thus avoiding regret.[44] The overlying *equity theory* suggests that especially when individuals are similar to each other, they compare the ratios of their contributions with the contributions of other people in their segment, and discontinue their relationship with a company if they perceive those ratios not to be equal.[45] In what can be considered one of the first and most prominent cases in which differential pricing was discovered, Amazon quickly stepped back from its experiment to charge customers different prices for DVDs after being subjected to heavy criticism and customer outrage.[46] Such evidence implies that it is not necessary for *every* customer to be sophisticated, as in the given example the presence of one customer with the necessary skills to uncover the practice sufficed to create enough pressure to provoke a change the price discriminating company's behaviour. The same kind of backlash can be faced by companies that charge a higher price for returning customers if the customers notice the change and subsequently turn their back on the firm.[47] Research on customers perception of price discrimination suggests that although they may not immediately abandon a firm they know to be price discriminating but are likely to exert more caution in future transactions with this firm.[48]

A final disincentive to personalise prices lies in the threat that customers may strategically choose to reject an initial price offer in the expectation of receiving a better offer in the future based on their experience with promotional pricing, which can hurt the firm in the long term.[49] These types of consumer reactions to price discrimination are

[44] Zuiderveen Borgesius and Poort, *op cit.*, p.356.
[45] Sarah Spiekermann, 'Individual Price Discriminaton in E-Commerce – An impossibility?', in: *Humboldt University Institute of Information Systems Research Paper* 2018, p. 2.
[46] Linda Rosencrance, 'Customer outrage prompts Amazon to change price-testing policy', *Computerworld*, 13 September 2000, Available at: https://www.computerworld.com/article/2597088/retail-it/customer-outrage-prompts-amazon-to-change-price-testing-policy.html (consulted on 7.4.2018)
[47] Cf. Acquisti, Taylor and Wagman, *op cit.*, p.17.
[48] Spiekermann, *op cit.*, p. 6.
[49] J. Villas-Boas, 'Price Cycles in Markets with Customer Recognition', in: *The Rand Journal of Economics*, Vol.35, No.3, 2004, p.487.

certainly less dependent on their knowledge of privacy-enhancing technology, however it can be argued that it is still doubtworthy whether they could fully suppress firm's incentives to price discriminate. In the given examples for such disincentives, a direct comparison between two price situations at two points in time was possible, which is a precondition that is unlikely to be fulfilled in the majority of the possibilities to exert price discrimination based on consumer targeting.

Another peculiar issue when it comes to price discrimination and behavioural targeting is the ever-growing importance of churn prevention. Especially industries such as telecommunication providers that are faced with high levels of customer attrition on the level of an annual 25-30% increasingly adopt strategic targeting mechanisms to identify valuable customers and prevent them from churning.[50] Traditionally, this is often conducted through a menu-based pricing approach[51] that gives customers the option to choose between different offers, making it a form of second-degree price discrimination. The availability of large amounts of data of customers has however given data processing companies the possibility to shift their churn-prevention efforts from a standardised offer segmentation to highly personalised targeting options for individual customers by applying methods such as decision-tree algorithms.[52] Among other examples, this highlights the ongoing trend for online business to get increasingly close to the formerly unattainable ideal of first-degree price discrimination.

The data economy is further marked by extensive customer-information sharing between companies, with digital data brokers selling access to extremely specific data to interested businesses.[53] Cross-selling customer data has been shown to be always profitable even between rival companies because the additional segmentation it enables for the less-informed business will not hurt the profits of the better informed one, making the trading a subgame perfect equilibrium that leads to an overall higher level of consumer surplus extraction.[54] There is an argument that consumers theoretically can avoid

[50] E. V. A. Ascarza, Raghuram Iyengar and Martin Schleicher, 'The Perils of Proactive Churn Prevention Using Plan Recommendations: Evidence from a Field Experiment', in: *Journal of Marketing Research (JMR)*, Vol.53, No.1, 2016, pp.46-47.
[51] *Ibid.*
[52] See for instance the application of Data Mining Techniques in an online casino environment in: Eunju Suh and Matt Alhaery, 'Customer Retention: Reducing Online Casino Player Churn Through the Application of Predictive Modeling', in: *UNLV Gaming Research & Review Journal*, Vol.20, No.2, 2016, pp.66-69, 75-76.
[53] George Norman, Lynne Pepall, Dan Richards and Liang Tan, 'Competition and consumer data: The good, the bad, and the ugly', in: *Research in Economics*, Vol.70, No.4, 2016, pp.752-753.
[54] Romain De Nijs, 'Behavior-based price discrimination and customer information sharing', in: *International Journal of Industrial Organization*, Vol.50, 2017, pp.320-321, 329.

businesses they know to be likely to trade their data and that there can thus occur competitive pressures that would force companies to choose between either giving offers at a lower or more personalised price or attracting customers through a more rigid privacy regime. Nevertheless, the extent to which the factors of a 'vote with the feet' or lower prices resulting from higher competition could mitigate the extraction of consumer surplus is rather low.[55] If the data of customers is however not shared or sold by the competing firms, they potentially end up worse off even if they acquire perfect information that enables them to first-degree price discrimination because the flow of such information increases competition in the product market.[56]

Regarding the welfare effects of online discrimination, the literature suggests that it might be beneficial to distinguish price discrimination that is pursued in the distribution of physical goods from differential pricing that is applied to digital goods (such as music or video games). While there is no indication that the welfare effects of the former would substantially differ from the remarks made in Section 3.1., some argue that first-degree price discrimination of digital goods might always have a positive welfare effect because their non-rival and non-excludable nature makes them comparable to public goods.[57] Since in a perfectly competitive environment the market price of such goods would approach zero, the high initial production costs could not be recovered by the producers, hampering investment and supply and thus making first-degree price discrimination socially desirable (and preferable to artificially raising market prices through intellectual property rights).[58] In the proposed pricing model, the customers would be substantially monitored by the distributing system and could after a trial period choose to pay for the digital good: Those with a willingness to pay that is higher than the price under uniform pricing would be 'refunded' the exceeding amount, whereas all customer with a willingness to pay below that threshold would pay the amount that was calculated to be their reservation price.[59] The scope of application of the model of 'mutually beneficial first-degree price discrimination' is arguably limited, as it applies only to digital goods that are repeatedly consumed and functions under the assumptions that (i) the customer monitoring is costless and accurate and that (ii) the arbitrage of manipulating one's personal data on the side of the customer comes at a cost that exceeds the benefits of the

[55] Norman, Pepall, Richards and Tan, *op cit.*, p.764.
[56] Chongwoo Choe, Stephen King and Noriaki Matsushima, 'Pricing with Cookies: Behavior-Based Price Discrimination and Spatial Competition', in: *Management Science,* pp.23-24.
[57] Thierry Rayna, John Darlington and Ludmila Striukova, 'Pricing music using personal data: mutually advantageous first-degree price discrimination', in: *Electronic Markets,* Vol.25, No.2, 2015, p.141.
[58] *Ibid.*
[59] *Ibid.*, pp.143-144.

manipulation. Nevertheless, such considerations highlight that it might be beneficial to review some of the basic assumptions on the welfare effects of both price discrimination and consumer privacy regarding the peculiar environment of the digital economy. An interesting remaining question is whether the tracking of internet users and the personalisation of prices could actually result in net welfare gains for both customers and producers in the presence of competition: As described above, competition between firms that have different degrees of information available about their customers can lead to those firms making fewer profits than under uniform pricing.

3.3. Sub-Conclusion

The traditional economic concept of price discrimination has been well adapted to the framework of online environments and their peculiarities such as the degree of information sharing, consumer preferences and traits of digital goods. Two insights are of particular relevance: First, the traditional argument that the general welfare outcome of price discrimination practices depends crucially on the type of price discrimination pursued by the company generally holds for the online environment. Second and more importantly, it becomes apparent that the information about online price discrimination that is available to customers and their corresponding behaviour crucially matter for the success of such measures. The extent to which information on consumers can be obtained and shared between suppliers ultimately determines whether a price discrimination approach can be profitable and is dependent on the capacity of the firm to obtain and use a sufficient amount of customer information, on the one hand, and the behaviour of customers, on the other hand. The potential impact of a regulatory privacy framework is consequentially dependent on the extent to which it (i) limits the information collection of companies and (ii) empowers individuals regarding the informational asymmetries vis-à-vis the price discriminating company.

4. Price Discrimination and Technology

Scholars have identified multiple criteria for defining successful personalisation activities. Firstly, there needs to be an adequate way of measuring the kind of effect that the matching customer traits with certain types of content has and a way of mitigation for possible measurement uncertainties.[60] Secondly, it is necessary that the user experience is not disturbed by the altering of the content through personalisation, and thirdly the computational methods deployed for establishing the link between customer data and content need to be scalable.[61] To enable such analyses, information about the customers' needs to be present. Generally speaking, information about consumers can be obtained in three ways: It can be (i) voluntarily and knowingly provided, e.g. by registering a user account, (ii) involuntarily and unknowingly obtained through online identifiers and (iii) obtained from third parties or the tracking of the customer's behaviour over multiple websites.[62] This section will provide insights into the technical aspects that enable price discrimination of customers, taking into account both the point of collection and the action of processing. Additionally, some ways of how privacy can be technically ensured in information systems will be briefly introduced.

4.1. Collection of Personal Data relevant to Price Discrimination

The following two sections will examine the most common ways of obtaining the personal data of individuals in online environments as well as some of the technical safeguards that can be applied to prevent such collection.

4.1.1. User Segmentation, Online Identifiers and Tracking Technologies

Information that can be used to price discriminate online can stem from a variety of sources. One of the most common ways to obtain information about individuals online are so-called 'Cookies', which are small text documents that are locally saved on a user's computer to save information about the user's characteristics and preferences and enable a personalisation of the web-content over the course of continuous interactions of the user with the web-page.[63] In contrast to 'Session Cookies' which get deleted after a user closes his browser, 'Persistent Cookies' are retained for future sessions and can, for example,

[60] Maurits Kaptein and Petri Parvinen, 'Advancing E-Commerce Personalization: Process Framework and Case Study', in: *International Journal of Electronic Commerce*, Vol.19, No.3, 2015, p.12.
[61] *Ibid.*
[62] Zuiderveen Borgesius and Poort, *op cit.*, p.351. As we will see in more detail in Section 4.2.1., this typology of information sources falls short of including methods of *inferring* (new) information on a customer by running probability estimations based on the existing data.
[63] Tobias Kollmann, *Definition: Cookie.* Gabler Wirtschaftslexikon, 2018, Available at: https://wirtschaftslexikon.gabler.de/definition/cookie-27577 (consulted on 24.03.2018).

ensure that the language chosen by the user or the customer's shopping cart history is displayed again on the website.[64] There is further a distinction between first and third party cookies: First Party cookies are placed by website publishers themselves, whereas third-party cookies are placed by parties other than the publisher, and can ascertain the identity of a user over multiple websites by using a unique code.[65] This 'tracking' of customers allows the displaying of multiple companies' content on a single website that appears to be edited by a single publisher but has, in reality, a modular structure. Third parties such as advertising networks can set their cookies on multiple of their partner websites, which enables them to recognise users on all websites part of that network and provide them with targeted content.[66] While such tracking cookies can still be deleted or opted out from, newer technologies such as Flash cookies can remain on a computer even after some basic clean-up operations have been pursued.[67] There is also evidence of companies using flash cookies that can re-install themselves after deletion, which is referred to as 'Zombie Cookies'.[68]

Other sources of identification and tracking do not necessarily rely on cookies. One example are the Internet Protocol (IP) Addresses of users, which uniquely identify a device on the internet or a local network[69] and can also be used to determine its geographical location. In the case of online price discrimination, it has additionally been shown that features such as the used browser or operating system are used to segment users into different categories that will receive different treatments on the website.[70] Taken alone, such features can only serve as a very basic and rough form of segmentation, as all users who are using the browser or operating system will get the same treatment, although their individual features might still be very different and not necessarily correspond to the third-degree price discrimination that would apply to them. However, there are also forms of identifier-less tracking that rely on the analysis of browser specifications such as the screen width or installed fonts, which is called 'device

[64] Frederik J. Zuiderveen Borgesius, 'Singling out people without knowing their names – Behavioural targeting, pseudonymous data, and the new Data Protection Regulation', in: *Computer Law & Security Review*, Vol.32, No.2, 2016, p.257.
[65] *Ibid.*, also see Article 29 Working Party, *A29WP Opinion 2/2010 on online behavioural advertising*, Brussels, 2010, p.6.
[66] Zuiderveen Borgesius, *op cit.*, p.257.
[67] Techopedia, *What is a Flash Cookie?* Available at: https://www.techopedia.com/definition/23464/flash-cookie (consulted on 5.4.2018).
[68] Zuiderveen Borgesius, *op cit.*, p.257.
[69] Per Christenssen, *IP Address Definition.* Tech Terms, 2018, Available at: https://techterms.com/definition/ip_address (consulted on 24.03.2018)
[70] Hannak, Soeller, Lazer, Mislove and Wilson, *op. cit.*, p.11.

fingerprinting'. A device fingerprint can be composed of a system of likely unique combinations of attributes and values[71], making it suitable for behavioural targeting.

While the technologies outlined above are certainly the most sophisticated ones to enable price discrimination against a certain individual, it is important to keep in mind that online price discrimination can also occur based on data that is related to other factors than individual traits. A classic example are airline tickets, whose prices can change significantly throughout the offer period based on two opposing forces: Prices initially increase the fuller the plane gets, but since airline tickets are a perishable good and the marginal costs of transporting another passenger are rather low, prices can decrease again if there are a lot of empty seats left. This strategy of *dynamic pricing* can have a price discriminating motivation, e.g. when the airline decides to increase prices again shortly before the departure date because it expects the remaining seats to be taken by business travellers with a high willingness to pay.[72] In these kinds of price discrimination settings, customers are charged different prices based on market data rather than based on data that is personal to them, other examples being the 'Surge Price Mechanism' deployed by Uber or the smart price algorithm of Airbnb.[73]

It can thus be stated that the type of price discrimination that can be deployed against online users depends crucially on the type of data that is analysed by the online companies. Where price discrimination relies on single identifiers such as the operating system or the point in time a user accesses a website, only a rough customer segmentation can take place that resembles third-degree price discrimination. In this way, online digital price discrimination would not essentially differ from traditional customer segmentation, e.g. when a franchise charges different prices in its brick and mortar stores depending on the geographical areas the shops are placed in. As shown above, individual features of users can, however, be digitally harvested and deployed to create user-specific profiles, hinting potentially at first-degree price discrimination.

---

[71] Gunes Acar, Marc Juarez, Nick Nikiforakis, Claudia Diaz, Seda Gurses, Frank Piessens and Bart Preneel, 'FPDetective: Dusting the web for fingerprinters', in: *Conference: Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security,* 2013, p.1131. A

[72] Marco Alderighi, Alberto A. Gaggero and Claudio A. Piga, *The hidden sides of 'dynamic pricing' for airline tickets.* LSE Business Review, 2017, Available at: http://blogs.lse.ac.uk/businessreview/2017/05/10/the-hidden-sides-of-dynamic-pricing-for-airline-tickets (consulted on 6.4.2017).

[73] Steppe, *op cit.*, p.775.

4.1.2. Privacy Enhancing Technologies and Privacy Protection by Design

The discussion on how to preserve privacy in online environments has accompanied the rise of the world wide web since the early stages of its development. In the late 1990's and early 2000s, the notion of Privacy Ensuring Technologies (PET's) gained popularity. It described technologies that aimed at "providing anonymity, pseudonymity, unlinkability, and unobservability of users as well as of data subjects".[74] Among the most important ones that are still in use and relevant to price discrimination are for instance cookie management and anonymisation technologies. Cookie management allows users to either disable cookies entirely, to select and allow only the cookies from providers they trust or to assess the information that a cookie will retain about them.[75] Anonymisation, in turn, refers to the use of a proxy to prevent the disclosure of the real identity of a user, deploying for instance specially configured firewalls or trusted third parties to serve as intermediaries in interactions and transactions of a user on the one side and a webpage on the other side. In general, PET's enable the customer to circumvent price discrimination (which may not be necessarily in his/her favour in case they had benefitted from the discrimination) or even to exert arbitrage to get a favourable discount.[76]

While such technologies grew more sophisticated with time, they still required and require a high level of awareness of the user, who must be capable of finding and using the respective programs to protect his/her privacy. Because of the low salience of data protection issues and low awareness of consumers about potential harms arising from a lack of privacy, lawmakers, as well as academics, increasingly became interested in the notion of 'privacy by design'. This approach aims at making information systems privacy friendly from the outset, without necessarily involving action of the user. The protection of personal data is thus supposed to be hard-coded into the informational architecture of a data processing service by designing environments in which estimations about the use of data for business purposes are made at the beginning rather than the end of the design process.[77] While it can be argued that privacy by design could have an economic value because its presence in the product can increase consumers trust into the company and can thus increase their loyalty,[78] it can also be assumed that it potentially reduces the

[74] Johannes Heurix, Peter Zimmermann, Thomas Neubauer and Stefan Fenz, 'A taxonomy for privacy enhancing technologies', in: *Computers & Security*, Vol.53, 2015, p. 2.
[75] Vanja Seničar, Borka Jerman-Blažič and Tomaž Klobučar, 'Privacy-Enhancing Technologies—approaches and development', in: *Computer Standards & Interfaces*, Vol.25, No.2, 2003, p. 154.
[76] Cf. Chapter 3, Section 3.2.
[77] Eric Everson, 'Privacy by design: Taking CTRL of Big Data', in: *Cleveland State Law Review*, Vol.65, No.1, 2017, pp. 28-29.
[78] Cf. the Apple case discussed in *ibid.*, pp. 40-41.

amount of data available to the company, making individualised price discrimination less feasible.

4.2. Big Data, Machine Learning and Artificial Intelligence

As mentioned earlier, the availability of data is not the only technological advancement that facilitates individual targeting since the large quantities of acquired information also need to be efficiently organised and analysed. The challenges posed by massive datasets is commonly referred to as 'big data', a term that can be defined as "high-volume, high-velocity and/or high-variety information assets that demand cost-effective, innovative forms of information processing that enable enhanced insight, decision making, and process automation".[79] In this definition, 'volume' describes the vast scale of the databases, 'velocity' refers to real-time data and 'variety' relates to the fact that the data can stem from very different types of sources.[80] The currently most advanced form of processing of big data systems is so-called 'machine learning', a process in which algorithms learn to identify patterns in the accumulated data and change their output accordingly.[81] Machine learning can occur either "supervised" in a process in which the algorithm learns to associate 'correct' correlations in a training data-set, or "unsupervised", which refers to a situation in which the algorithm autonomously seeks patterns in the data without an indication what to search for.[82] This problem-solving capacity that is acquired by the algorithms is a form of Artificial Intelligence (AI), which (although often used interchangeably) refers more generally to the capability of a computer to model an aspect of the world and apply that model to future scenarios.[83] The combination of the concepts of AI, machine learning and big data is finally what we call 'big data analytics'.[84]

The process of big data usage can be divided into three phases: Acquisition, analysis and application.[85] The acquisition phase is marked by a compiling of data that can be

[79] Gartner IT Glossary, *What Is Big Data?* Available at: https://www.gartner.com/it-glossary/big-data (consulted on 4.3.2018).
[80] Information Commissioner's Office, *Big data, Artificial Intelligence, Machine Learning and Data Protection*, Wilmslow, 2017, p.6.
[81] *Ibid.*, p.7.
[82] *Ibid.*, pp. 7-8.
[83] *Ibid.* pp.6-7.
[84] *Ibid.*, p.9.
[85] The corresponding three-phase model is proposed by Manon Oostveen, 'Identifiability and the applicability of data protection to big data', in: *International Data Privacy Law*, Vol.6, No.4, 2016, pp. 300-302. Note that this model is purposively simplistic and adapted to legal evaluations, leaving out some differentiations that are irrelevant in legal contexts.

directly obtained from consumers in the course of registration or tracking (cf. section 4.1.1.), bought from third parties or collected from publicly available sources. Finally, big data analytics also result in the creation of new data by recognising patterns that can then again be part of the amassing of data in the acquisition phase. In the analysis phase, this data is then, often in anonymised form, stored or processed with the aim of creating inferences and hypotheses by finding correlations and patterns.[86] In the application phase, the created models are then applied to individuals, either by directly targeting them or affecting them as a member of a group that is affected by the calculated outcome.

4.2.1. Big Data Analytics Implications for Online Price Discrimination

In its analysis of big data analytics, the Information Commissioner's Office of the United Kingdom establishes five features that distinguish big data analytics from hitherto processing, scilicet (i) the use of algorithms, (ii) the opacity of the processing, (iii) the tendency to collect 'all the data', (iv) the repurposing of data, and (v) the use of new types of data.[87] In the following, it will be briefly outlined how the combination of those features allow for some sophisticated techniques of profiling that could be harnessed for price-discrimination practices.

While algorithms as such are not a new phenomenon, the possibility to use of them as complex neural networks has vastly accelerated due to advances in computational power. In neural networks, single algorithm units in a bottom layer combine input values to produce an output value that is subsequently passed on to individual or multiple units up in the next layer, resulting in a synapse-type of computing that may sometimes entail more than 100 layers, resulting in highly complex and precise outcomes.[88] Thus, such networks are essentially modelled on the functioning of the human brain. Although they are still far from achieving the status of a 'general AI' that would achieve human-like intelligence and adaptation capabilities throughout a wide variety of tasks, 'narrow AI' applications can easily surpass human pattern and correlation recognition in highly specific tasks and perform extremely well at routine types of jobs.[89]

The enormous pattern recognition capacity of machine learning allows in theory for an extremely detailed segmentation of customers based on a vast array of traits. Whether

---

[86] *Ibid.*
[87] Information Commissioner's Office (Big Data Report), *op cit.*
[88] Executive Office of the President; National Science and Technology Council; Committee on Technology, *Preparing for the Future of AI,* Washington D.C., 2016, pp. 9-10.
[89] Ben Dickson, 'What is Narrow, General and Super Artificial Intelligence?', *TechTalks*, 12th May 2017, Available at: https://bdtechtalks.com/2017/05/12/what-is-narrow-general-and-super-artificial-intelligence (consulted on 16.4.2018)

a capitalisation based on such ever more granular grouping strategies is ethical is however a troublesome question, especially if certain features that influence a pricing decision correspond closely to ethnicity, sexual orientation or gender.[90] This is problematic because the immense complexity of big data analytics outputs also come with a high degree of opacity that essentially makes the decision making process a "black box" in which it takes considerable effort to understand a particular outcome, which is sometimes almost impossible even for experienced AI scientists.[91] In terms of personalised pricing, this poses essential problems regarding the threat of discrimination since the extremely granular analyses of customer sections will with a high probability incorporate and use traits of customers that respond to their ethnicity, gender or sexual orientation.[92] Far from the hope that automated systems might eradicate the biases of human perception, algorithms based on such data may reproduce those biases because they are incorporated in their human-programmed coding or because the data they are fed with is inaccurate or biased.[93] Furthermore, because big data can draw potentially privacy intrusive inferences from the combination data points that taken individually are originally not privacy sensitive, big data analytics have the potential to circumvent the traditional three elements of privacy legislation, scilicet collection, processing and disclosure.[94] In regard to personalised pricing, this suggests that it might become impossible for individuals to prevent price-discrimination against them, because even if they opt-out from sharing data that they regard as vital for such practices other freely available data entries related to them might in combination reveal the same insights. While this is already potentially problematic for consumers in general, the issue becomes exacerbated when it comes to groups with a special vulnerability. Even if both the data that is entered and the algorithm computing the outcome are 'objective', and no discriminating categories such as race or gender are used for the output-estimation, the automated decision can still be discriminating against a certain group because the interlinking of different points of data can result in a profiling of traits that serves as a 'proxy' to the special categories data.[95]

---

[90] Cf. Michael Schrage, 'Big Data's Dangerous New Era of Discrimination', *Harvard Business Review*, 29 January 2014, Available at: https://hbr.org/2014/01/big-datas-dangerous-new-era-of-discrimination (consulted on 25.4.2018).
[91] Davide Castelvecchi, 'Can we open the black box of AI?', in: *Nature News*, Vol.538, No.7623, 2016, pp. 3-4.
[92] Schrage, *op cit.*.
[93] Danielle Keats Citron and Frank Pasquale, 'The scored society: Due process for automated predictions', in: *Washington Law Review*, Vol.89, No.1, 2014, pp.4-5.
[94] Kate Crawford and Jason Schultz, 'Big Data and Due Process: Toward a Framework to Redress Predictive Privacy', in: *Boston College Law Review*, Vol.55, No.1, 2014, p.106.
[95] Anupam Datta, Matt Frederikson, Ko Gihyuk, Piotr Mardziel and Sen Shayak, 'Proxy Discrimination in Data-Driven Systems', in: *Theory and Experiments with Machine Learnt Programs*, 2017, p.3.

A simple example of such indirect discrimination or 'proxy discrimination' would be for instance that an automated decision based on the ZIP code of a certain geographical area can be discriminating because this area is primarily inhabited by a certain ethnicity, which has in the past already been a problem in Amazon's policy to not supply its same-day delivery service to predominantly black neighbourhoods.[96] In the black-box analysis phase of big data analytics, where a vast array of different data types might be used to generate a decision, the question whether or not discrimination against a certain group took place becomes thus obviously much harder to evaluate.

Lastly, big data analytics may not only be used to anticipate a consumer's willingness to pay but also to *shape* it according to the need of the supplier. This capacity is described by the notion of 'nudge', meaning the designing of choice architectures in a way that makes humans prefer one choice over another by applying insights from behavioural psychology.[97] While nudges have arguably been in use for a long time (e.g. when a supermarket places the more expensive items on the eye-level of a customer and while the less profitable ones are put in segments that are harder to reach), big data analytics give this demand shaping capacity a new quality. Because the analysis of real-time data flows allows for (i) a refinement of the customer's choice environments according to their monitored behaviour, (ii) the continuous creation of new data that can be stored and repurposed for other big data applications and (iii) the application of obtained knowledge about general, population-wide trends to the individual customers' choice architecture, the subtle shaping of online choice environments becomes personalised to an extent that has been called 'hypernudge'.[98] The availability of excessive amounts of data on a customer combined with the capability to influence his decision making thus goes beyond making decisions based on knowledge about his willingness to pay, it is the exploitation of the individuals' traits to *create* a certain willingness to pay. Companies could thus increasingly resort to "create [their own] suckers, rather than waiting for one to be born".[99]

---

[96] David Ingold and Spencer Soper, 'Amazon Doesn't Consider the Race of Its Customers. Should It?', *Bloomberg*, 21st April 2016, Available at: https://www.bloomberg.com/graphics/2016-amazon-same-day (consulted on 16.4.2018).
[97] Karen Yeung, ''Hypernudge': Big Data as a mode of regulation by design', in: *Information, Communication & Society*, Vol.20, No.1, 2017, p. 120.
[98] *Ibid.*, p.121.
[99] Ryan Calo, 'Digital Market Manipulation', in: *George Washington Law Review*, Vol.82, No.4, 2014, p.1018.

4.2.2. Big Data Analytics as a Way of Mitigating Price Discrimination

While big data analytics can in the ways outlined above certainly unfold an enormous potential to personalise online environments, including both pricing and choice architecture and might thus contribute to an increase in consumer surplus extraction, there also exist approaches that might serve as mitigation for price discrimination. In the following, they will be briefly outlined to explore ways in which big data analytics can work less privacy intrusive even in the absence of regulation.

Regarding proxy discrimination, it might be possible to filter not only the special categories data as such from the algorithm decision making but also their proxies. To this extent, the model needs to be trained by computing both how closely certain data points are related to an attribute like gender and how important those data points are in the decision-making process. If those points then exceed a certain threshold, they are also obstructed from the model.[100] This may pose an effective way of mitigating potential discriminatory harm, but while this approach is certainly a step forward and would prevent cases like the Amazon ZIP code one discussed above, it might still not completely rule out proxy discrimination in cases where it is not single values that indicate the individual's protected trait and could subsequently take the established threshold, but the *combination* of those values that leads to the discrimination.

Another way of how big data analytics could potentially mitigate price discrimination would be the deployment of algorithms as bargaining agents for consumers. The deployment of autonomous negotiation algorithms could potentially be applied to bargain about the usage of sensitive data and could thus help to achieve a satisfying trade-off between the privacy concerns of a customer on the one hand and his/her willingness to accept a higher price or reduced convenience on the other hand.[101] However, there are currently no such technologies available and a lot of additional research will be necessary, not least to address the ethical questions related to the matter such as whether the algorithm should be allowed to intentionally provide on behalf of the customer to achieve a more beneficial outcome.[102]

---

[100] Datta, Frederikson, Gihyuk, Mardziel and Shayak, *op cit.*, pp. 9-10, p. 13.
[101] Tim Baarslag, Michael Kaisers, Catholijn M. Jonker, Enrico H. Gerding and Jonathan Gratch, 'When Will Negotiation Agents Be Able to Represent Us? The Challenges and Opportunities for Autonomous Negotiators', in: *Twenty-Sixth International Joint Conference on Artificial Intelligen*, Melbourne, 2017, p. 4684.
[102] *Ibid.*, p. 4689.

4.3. Sub-Conclusion

From the above sections, it becomes apparent that the personal data of customers can be retrieved and analysed in ever more sophisticated ways. Many of the tracking practices that are possible to be pursued to obtain information about an individual are highly opaque and make an informed choice or trading of one's data a very difficult undertaking that may take a sophisticated knowledge of PET's. The analysis of the acquired data in contrast is not only potentially illusive for the price discriminated customer, but even to the price discriminating supplier him/herself. This gives rise to the legitimate concern about indirect discrimination of sensitive customer groups, as neither the ethical proportionality of a price differentiation based on such segments in general nor the line between legitimate profit maximisation and harmful discrimination are sufficiently clear. It can thus be stated that the criteria for a regulatory framework to have an impact on the issues identified above are (i) the width of data categories that are captured by the regulation, (ii) the extent to which it requires an algorithmic decision to be transparent and (iii) the objection and rectification measures it offers to individuals.

5. Analysis: Inferences on Price Discrimination from the General Data Protection Regulation

The General Data Protection Regulation (GDPR) will have a profound impact on the ways in which personal data can be stored and processed in the EU in the future, as it applies to all companies that operate in the Union.[103] Since compliance with the regulation is thus not bound to the geographical location of a company but to the geographical location of its *activity*, it can be assumed that the regulation will produce significant effects not only within the Union but everywhere where the data of EU citizens is processed, which gives it the potential of achieving a global impact.[104] Furthermore, the nature of the legislation being a regulation rather than a directive (such as the previous data protection framework of Directive 95_46_EC) means that it will bring a substantial harmonisation effect in the EU digital single market, since its provisions will equally apply in all member states without the need to be transposed into national law. It updates existing concepts such as user consent and introduces newer forms of data protection, such as the 'right to be forgotten' principle. In the following, the provisions of the GDPR will be matched with the findings from the previous two chapters. They will be underlined by the practical example of the chosen case study; the enterprise of Darwin Pricing. The main findings will subsequently be synthesised in the chapter's sub-conclusion.

5.1. The Material Scope of the GDPR and its Applicability to Price Discrimination

Personal data as defined by the GDPR refers to "any information relating to an identified or identifiable natural person ".[105] Natural persons need to be distinguished from legal persons, who are not subject to the scope of the GDPR. This has been interpreted as a potential loophole in terms of price discrimination, as the harnessing of legal undertakings' name and form, as well as their contact details, might in certain circumstances put them at an equal risk to be discriminated against as natural persons, e.g. when their annual accounts are retrieved online.[106] In the interpretation of the Article 29 Working Party, the term 'any information' is considered to be required to be interpreted widely, including both 'objective information' such as health data and 'subjective data' which relates to

[103] General Data Protection Regulation, *op cit.*, Art.3.
[104] Consider for instance the analysis of Mark Scott and Laurens Cerulus, 'Europe's new data protection rules export privacy standards worldwide', *Politico Europe*, 31 January 2018, Available at: https://www.politico.eu/article/europe-data-protection-privacy-standards-gdpr-general-protection-data-regulation (consulted on 28.3.2018).
[105] General Data Protection Regulation, *op cit.*, Art. 4 (1).
[106] Steppe, *op cit.*, p.773.

opinions and assessments.[107] That subjective information is covered by the GDPR as well is significant for two reasons: Firstly, assessments of for example a customer's creditworthiness might in certain circumstances be even more revealing than 'objective' data points, as the latter can involve a necessity for an extensive 'connecting of the dots' to allow inferences on a certain characteristic of an individual (which does, however, become increasingly simple by applying measures of big data and artificial intelligence). Secondly, such assessments may in certain contexts be especially prone to be used as a basis for price discrimination. However, sensitivity is not a required feature to qualify data as personal, as information on whatever kind of activity that is undertaken by an individual will be necessarily captured by the definition.[108] In regard to price discrimination, both predictive profiling of customers based on online behavioural observation and user-generated profiles where individuals fill in registration forms etc. will, therefore, be covered by the GDPR.[109] In a similar way, data that can be used for market segmentation of customers will likely be 'related' to individual persons in the legal sense of the regulation: The fact that such practices rely on estimations of the wealth or other price sensitivity indicating features of customers and aim at differentiating the prices charged to them can be logically assumed to have an impact on the individuals' rights and interests, which lets this data fall within the scope of the Article 29 Working Party's considerations regarding personal data.[110] The three elements that can respectively be applied to establish a link between an individual and certain data entries, scilicet *content* (the data is about an individual), *purpose* (the data is used or likely to be used to evaluate or influence the status or behaviour of an individual) and *impact* (the use of the data is likely to have an impact on an individual's rights and interests)[111] do indeed cover a vast range of data forms and thus demands special consideration regarding online price discrimination techniques.

Concerning the criterion of identifiability, any data that makes it possible to directly or indirectly identify a natural person by making it possible to distinguish a natural person within a group from all other members of that group is affected by the GDPR.[112] While

---

[107] Article 29 Data Protection Working Party, *A29WP Opinion 4/2007 on the concept of personal data* Brussels, 2007 p.6.
[108] *Ibid.*, pp.6-7.
[109] Cf. Steppe, *op cit.*, p.773.
[110] *Ibid.*
[111] Article 29 Data Protection Working Party (Opinion 4/2007), *op cit.*, pp.10-11.
[112] *Ibid.*, p.12. The Article 29 Working Party is an advisory body composed of representatives of national data protection authorities, cf. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Art. 29, 30.

'direct identifiability' most commonly refers to an individual's name, 'indirect identifiability' is context specific and depends on "unique combinations" of a number of identifiers that may allow an inference to the identity of a given individual.[113] In principle, this extends the scope of the GDPR to analyses and decisions that can be derived from big data analytics even if the data points as such comprise non-personal data but can single out an individual when they are regressively combined. This makes the material scope of the GDPR highly comprehensive and would capture even techniques such as device-fingerprinting (c.f. section 4.1.1.). However, the emphasis on a *combination* of such points might not be beneficial in all circumstances, given that even in an anonymised set of a single type of data, individuals can potentially be singled out and made identifiable compared to all other members of the group, which was for instance demonstrated in the example of human mobility traces.[114] This raises the question whether it will be possible to maintain the distinction between anonymous or non-identifiable data and personal data in the future, or at least whether a more granular approach to the risk management of identifiability will need to be adopted at some point. To some extent, this issue is reflected in Recital 30 of the regulation which acknowledges that the traces left by online identifiers may be associated with natural persons. The formulation that user profiles could be created from such traces "in particular when combined with unique identifiers"[115] is a potential hint that a combination with identifiable data is not an exhaustive or absolute requirement for making the GDPR apply to non-personal data. In any case, the current standing interpretation of identifiability does not consider this matter, but it is on the other hand not inconceivable that future jurisprudence of the CJEU will bring more clarity in this regard.

The above considerations were to some degree present in the judgement of the CJEU to regard dynamic IP-Addresses as personal data, which has been regarded as a landmark decision regarding the material scope of EU data protection legislation.[116] Although less privacy intrusive than static IP addresses, which do not change when starting a new session of connection to the internet and are generally considered to be personal data,[117] dynamic IP addresses can still constitute personal data in the jurisprudence of the CJEU

[113] Article 29 Data Protection Working Party (Opinion 4/2007), *op cit.*, p.13.
[114] Yves-Alexandre De Montjoye, César A. Hidalgo, Michel Verleysen and Vincent D. Blondel, 'Unique in the Crowd: The privacy bounds of human mobility', in: *Scientific Reports,* Vol.3, 2013, p. 4.
[115] General Data Protection Regulation, *op cit.*, Recital 30.
[116] See for instance Marcin Kotula, *IP addresses as personal data - the CJEU's judgment in C-582/14 Breyer*. EU-Law Analysis, 2017, Available at: https://eulawanalysis.blogspot.com/2017/01/ip-addresses-as-personal-data-cjeus.html (consulted on 3.4.2018).
[117] Article 29 Data Protection Working Party (Opinion 4/2007), *op cit.*, p.15.

when the internet service provider has the legal means to identify the data subject with additional data that is also available to the provider.[118] The significance of the judgement lies however also in its definition of the threshold of identifiability under the involvement of third parties, for which the court stated that identifiability would not be present if the "identification of the data subject was prohibited by law or practically impossible on account of the fact that it requires a disproportionate effort in terms of time, cost and man-power, so that the risk of identification appears in reality to be insignificant"[119] This argumentation is based on the assumption that the distinction between personal data and non-personal data would entirely blur if the hypothetical threat of a later identification of the data subject through third party data would always be treated as an unlimited ground to classify data as capable of identification.[120] In the context of big data, it might be appropriate to ask what the boundary of a 'disproportionate effort' may be, given that the combination of non-identifiable datasets with sets including personal data is fairly easy for an acquiring party using advanced algorithms and given that the trade with datasets is continuously flourishing.[121] As stated earlier, the reliance of the current jurisprudence and the GDPR on making identifiability dependent on keeping the different types of data separated from each other may in the end not be extensive enough to prevent individualised profiling.

Data that is used in the course of price personalisation will furthermore fall under the GDPR definition of 'processing' as "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction".[122] It will thus not matter whether the data that could indicate a consumers price elasticity was obtained through wilful disclosure by the data subject or through an automated process on the website. Additionally, it has been pointed out that not only the price discriminating supplier himself will be subjected to the GDPR, but also third parties that read cookies or other browser related data to offer price discounts in advertising and link to the supplier's website.[123]

---

[118] CJEU, *C-582/14 Breyer v Bundesrepublik Deutschland*, 2016, para. 49.
[119] *Ibid.*, para. 46.
[120] Cf.. Steppe, *op cit.*, p. 774 in his recital of Advocate General Campos Sanchez-Bordona.
[121] Oostveen, *op cit.*, p. 306.
[122] General Data Protection Regulation, *op cit.*, Art.4 (2).
[123] Cf. Steppe, *op cit.*, p.776

The extensive material scope of the GDPR thus appears to capture most of the data that is relevant to price discrimination, especially concerning personalisation on an individual level. This fulfils the proposition of the necessary scope a privacy legislation would need to have to have an impact on online price discrimination that was set up in the section of 4.3. It also fits the previous estimation of the Article 29 Working Party regarding the application of the former directive 95/46/EC to behavioural targeting, which it considered as given in the majority of cases.[124] While more rough discrimination based on browser, operating system, aggregate data about geographical areas and other types of data that enable a segmentation without identifying natural persons will in turn not be affected, it should be kept in mind that the prospects for profit increases are much lower in those cases and that those types of data will still count as personal data as soon as a company would link the trait to an established customer profile.[125] This appears to be relevant for big data analytics as well: Given that data that can be directly linked to a user always qualifies as personal data, the connection of data points that are in their original form not privacy intrusive will subject all this information to the GDPR provisions if the outcome relates to an identifiable person, potentially affecting large parts of a given big data set.

5.2. Principles relating to Processing

The second chapter of the GDPR introduces a number of principles relating to the processing of personal data, of which a number have implications for online price discrimination. In the following, some observations regarding the lawfulness of processing, the consent procedures for consumers, the processing of special categories of data and processing which does not require identification will be made.

5.2.1. The Lawfulness of Processing

Personal data must be "processed lawfully, fairly and in a transparent manner in relation to the data subject" under the GDPR.[126] The changes introduced regarding the lawfulness of processing have been considered as some of the most significant ones, and many privacy professionals from the EU and the United States (US) regard it as one of the areas

[124] Article 29 Working Party (Opinion 2/2010), *op cit.* p. 9.
[125] Zuiderveen Borgesius and Poort, *op cit.*, p. 359.
[126] General Data Protection Regulation, *op cit.*, Art. 5 (1 a).

that are most endangered of non-compliance.[127] and the strict requirement for processing to fall into one of the stated legal justifications is seen as a substantial raising of the bar compared to previous standards.[128] Regarding online price discrimination, the provisions of data subject consent, processing in the context of a contract and processing for the purpose of a legitimate interest of the controller or a third party are the most likely bases for a lawful processing of customer data.

Consent is undoubtedly one of the most heatedly debated issues in the context of the GDPR. In the regulation, consent of a data subject is defined as "any freely given, specific, informed and unambiguous 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".[129] In its latest guidelines on consent, the Article 29 Working Party regards 'freely given' as an unsatisfied condition if there are negative consequences or detriments connected to a denial of consent or if there is, in general, no real choice, especially when consent is demanded for the provision of data that is not expressly necessary for the provision of the service.[130] Similarly, it is no longer possible to 'bundle' or 'tie' consent with the acceptance of a contract or terms of conditions, as it is considered not to be freely given when the contract allows the contracting party to obtain data that is not necessary for the performance of the contract.[131] Regarding current practices of achieving consent, those provisions are likely to require a significant change, as the widespread approach of 'implied consent' where using the website or service is counted as consent to all forms of data collection will need to be substituted by a written or oral statement, or at least the ticking of a box or an initial choice of settings before using the service.[132] Thus, processing operations that rely on customer consent will need to become more granular, as all purposes for which data may be processed will need to be agreed to by the customer on a case by case basis.[133] It must further be possible for individuals to withdraw their consent at any given point in time, which will however not make the processing of the data before the withdrawal unlawful.[134] Finally, the GDPR

---

[127] In the survey presented by IAPP, *Geting to GDPR Compliance: Risk Evaluation and Strategies for Mitigation,* Portsmouth, 2018, p. 4, obtaining consent was considered to be third among the most risky elements of non-compliance according to the 500 respondents queried.
[128] Consider for instance the assessment of DLA Piper Global Law Firm, *EU General Data Protection Regulation - Key changes* Available at: https://www.dlapiper.com/en/uk/focus/eu-data-protection-regulation/key-changes/#higher%20bar (consulted on 26.5.2018).
[129] General Data Protection Regulation, *op cit.,* Art. 4 (11).
[130] Article 29 Working Party, *Guidelines on consent under Regulation 2016/679,* pp. 5-6.
[131] General Data Protection Regulation, *op cit.,* Art. 7 (4), Recital 43.
[132] *Ibid.*, Recital 32.
[133] Cf. *Ibid.*, Recital 43.
[134] Steppe, *op cit.*, p. 777.

also holds suppliers liable not to be ambiguous about the purposes for which the personal data is processed. Consent must be informed by written, oral, audio or video communication, and the language used must be understandable for an average member of the addressed group.[135] The purposes for which the data is going to be processed further need to be clearly stated and the affirmative act of the individual must leave no reasonable doubt that there is a deliberate wish to allow the processing.[136]

The combination of having to clearly and unambiguously inform individuals, enabling them to choose their consent on a case by case basis depending on the purpose of the processing and the prohibition of detrimental treatment could have a significant impact on price personalisation and targeting. A webshop could, for instance, not coerce users into providing consent by making it impossible to use the shop in case the customers do not agree to be price discriminated. Since the primary function of an e-commerce offer is likely to be the provision of goods, the minimum consent that a user needs to give for using the service will need to be directly linked to data that is strictly necessary for the shop's functioning, e.g. the storage of login or payment data. This also means that the widespread 'tracking' of users as discussed in Chapter 4.1. will need to come under the data subject's scrutiny: Website owners will be liable for the processing of third-party cookies that they implement into their website architecture, which would require them to be informed in detail about the ways in which this data is used in order to pass this knowledge on to consumers adequately. This could prove difficult, and many providers will be dependent on the way large advertising networks handle the issue.[137] In any case, website owners who seek to personalise prices for customers based on data they acquire through tracking will need to notify users about both the tracking activity and price discrimination aim, regardless of whether the data is acquired through their own or third-party technology.

Given the extensive necessity to obtain consent from customers, which gives them a deeper choice regarding which data of them is processed and for what purpose, the impact criterion of *behavioural empowerment* that was defined in section 3.3. is comprehensively satisfied by the regulation. The most interesting question arising in this context is what the practical implications of this stricter handling of customer opt-ins are going to be. As elaborated in section 3.2., price discrimination is highly contested among consumers and

[135] Article 29 Working Party (GDPR Guidelines on consent), *op cit.*, pp. 13-14. Also see Article 29 Working Party, *Guidelines on Transparency under Regulation 2016/679*, Brussels, 2018, p. 40.
[136] Article 29 Working Party (GDPR Guidelines on consent), *op cit.*, pp. 15-16.
[137] Bozhidar Bozhanov, *Tracking Cookies and GDPR*. 2018, Available at: https://dzone.com/articles/tracking-cookies-and-gdpr (consulted on 29.4.2018).

companies that become known for having price discriminated face high degrees of customer backlash. While empirical research on whether and how customers are going to make use of the new consent architecture will only be possible after a sufficient amount of time after the entry of the GDPR, some estimations are possible to be derived from economic theory. As stated earlier, regret aversion and equity theory suggest that customers will be increasingly cautious in transactions with price discriminating companies and may even stop buying there if they fear to pay more than members of their peer group, which would imply that many consumers would deny or withdraw their consent to be price discriminated if presented with a clear and obvious choice for doing so. This would, in turn, lower the profits of the enterprise in two potential ways: Firstly, less price discrimination opportunities suggest less consumer surplus extraction and thus reduced profits, which constitutes an impact on societal welfare of the regulation. Secondly, the overall amount of data available to the training of the price discriminating algorithms would be reduced, potentially resulting in less accurate consumer targeting, which can be seen as a *behavioural empowerment impact on the technical implementation of online price discrimination.* The latter is, however, rather unlikely given that data for training purposes can also be acquired from third parties and considering that many price personalisation solutions are anyway offered by third parties who provide readily trained algorithms for the customer companies' data records.[138] Both of the stated adverse effects on online price discrimination could be mitigated or even potentially reversed when price discrimination occurs as part of a discount strategy, which is likely to be perceived less negatively by consumers.[139] While it has been found that the strategy of 'couponing' (meaning the distribution of promotional codes that can be redeemed on the website) is often detrimental in online environments because customers who do not have a coupon might leave the shop or because only tech-savvy users make use of them,[140] discounts can also be given based on targeting users through online identifiers. For instance, discounts can be charged to users who visit the website for the first time, who would likely opt-in to be recognised as first-time customers if the information given on the website promises

[138] See as two examples for instance the offers of Darwin Pricing or SPOSEA Europe: *Dynamic Pricing Software for Geo-Targeted eCommerce.* Available at: https://www.darwinpricing.com/de/geo-targeted-ecommerce (consulted on 27.4.2018), *BrightPrice Suite.* Available at: http://www.sposea.com/bright-price-suite.html#pdm (consulted on 27.2.2018).

[139] Cf. Harlan Landes, 'Individualized Coupons Aid Price Discrimination', *Forbes*, 21 August 2012, Available at: https://www.forbes.com/sites/moneybuilder/2012/08/21/individualized-coupons-aid-price-discrimination/#26c20f8a45e7 (consulted on 27.4.2018).

[140] Mikhael Shor and Richard L. Oliver, 'Price discrimination through online couponing: Impact on likelihood of purchase and profitability', in: *Journal of Economic Psychology*, Vol.27, No.3, 2006, p. 437, Richard L. Oliver and Mikhael Shor, 'Digital Redemption of Coupons: Satisfying and Dissatisfying Effects of Promotion Codes', in: *Journal of Product & Brand Management*, Vol.12, No.2, 2003, p. 131.

a price discount in exchange for placing a cookie that will recognise them in the future. While the remaining risk of users deleting their cookies and subsequently reaping the benefits of the first-time discount through continuous utilisation of the offer is likely to be low given the low number of people who regularly reset their browser cookie profiles,[141] such strategies are an example of how companies could convince users to allow the processing of their data for price discrimination purposes.

Another possible scenario is that the new consent procedures might create barriers to market entry because adopting technologies that enable the individualised provision of consent are costly and because users may prefer to give consent to companies they are familiar with.[142] This would constitute potential competition detriments as big firms would be more likely to acquire data, giving them not only a better chance to price discriminate in general but also to acquire more precise algorithms.

The importance of the above considerations is underlined by the fact that the GDPR strictly forbids the use of the collected personal data for other uses than the ones the data was originally collected for.[143] The rather vague information that is currently often provided in e-commerce, e.g. "personalising the user experience" has thus correctly been described as overly broad and not suitable for obtaining purpose limited and informed consent, not to speak of instances where automatic targeting occurs based on geolocation or operating system.[144] Apart from such imminent operational changes price discriminating businesses will thus need to go through, consent also becomes a difficult issue in the context of big data: Because the use and application of the data are ultimately impossible to predict in big data analytics, the binary choice of opting in or opting out in such an opaque environment might become a misguided principle in the future.[145] In this regard, suggestions have been made by the European Union Agency for Network and Information Security (ENISA) to explore models of automated consent, deploying for instance software agents that give consent on behalf of the user based on certain properties or relying on certain user actions such as behavioural patterns.[146] Other proposals include the option that companies should explicitly state to users that their non-specified data can

[141] Cf. the previously cited statistic by Privacy and protection of personal information *op cit.*
[142] James Campbell, Avi Goldfarb and Catherine E. Tucker, 'Privacy Regulation and Market Structure', in: *Journal of Economics & Management Strategy*, Vol.24, No.1, 2015, pp. 67-77.
[143] General Data Protection Regulation, *op cit.*,Art. 5 (1 b)
[144] Steppe, *op cit.*, pp. 777-778.
[145] Information Commissioner's Office (Big Data Report), *op cit.*, p. 30
[146] Giuseppe D' Acquisito, Josep Domingo-Ferrer, Panayiotis Kikiras, Vicenç Torra, Yves-Alexandre De Montjoye and Athena Bourke, ENISA, *Privacy by Design in Big Data. An Overview of Privacy Enhancing Technologies in the Era of Big Data Analytics.*, Heraklion, 2015, p. 46.

be used to make predictive statements about them[147] or try to explain them in the best way possible the potential benefits of agreeing to their data being processed in the course of big data analytics and thus obtaining consent.[148] However, it remains difficult to imagine that such practices would count as informed consent to a full extent since neither the type of data nor the ultimate use of it can be specified at the time of obtaining consent. On the other hand, it is also possible to imagine situations in which personal data created in the course of the analysis stage can still serve the purpose for which it was originally created. A user could, for instance, agree to have his scrolling behaviour logged in exchange for receiving preferential price offers, which the supplying firm originally intends to use to detect and mitigate the risk of churn. If the data is however processed further to reveal additional features of the customer that can be used to place him in a certain market segment, and this newly created data is again used to provide even more targeted price offers, the purpose of the original data point has not changed. Such practices may, however, become problematic in the course of profiling and regarding special categories data, which will be outlined in subsequent sections.

A final, highly interesting question is to what extent suppliers will need to ask customers for their consent regarding the adaptation of their choice architectures according to the collected behavioural data (cf. Chapter 4.1.). After all, adapting a website to the specific customer can have a significant impact on his/her purchasing decision.[149] The provision for informed consent can however not be interpreted to go as far as obliging website owners to make this purpose explicit, especially because it would be hard to distinguish an adaptation that is aimed at influencing the purchasing decision from general adjustments implemented for the user's convenience. While consent to the personalisation of a webshop's architecture as such will be required under the GDPR, customers will likely neither know nor be informed about the fact that their consent also allows for a potential erosion of their autonomy in their purchasing decision. On a different note, individuals could further be 'nudged' to provide consent in the first place. For the health sector, using nudges to obtain patients informed consent to certain treatments has for instance been proposed as a useful way of increasing the patient's welfare.[150] In regard to online price-discrimination, there would clearly be an (less ethically motivated) incentive to build choice architectures according to the wish of the

[147] Article 29 Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, Brussels, 2017, p. 22.
[148] Information Commissioner's Office (Big Data Report), *op cit.*, p.31.
[149] Kaptein and Parvinen, *op cit.*, p. 9.
[150] Shlomo Cohen, 'Nudging and Informed Consent', in: *The American Journal of Bioethics*, Vol.13, No.6, 2013,

supplier to obtain the consent of as many people as possible to receive personalised price offers. If successful, such nudges could thus increase the amount of customer information obtained by online businesses for price personalisation purposes.

Contractual and Pre-Contractual Measures have also been discussed as a possibility to achieve lawfulness of processing in relation to online price-discrimination. The condition for lawfulness is satisfied if the processing of personal data is "necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract".[151] The pivotal issue in this regard is the degree of necessity, which has been argued not to be present for discriminatory pricing because although a pricing decision can be seen as a necessary precondition for entering into a contract, such a decision is possible as well under linear pricing.[152] Equally, browsing a website cannot be regarded as a contractual relationship as such, and even if a purchase has been concluded in the past, the contractual relationship established on this ground does not entail a necessity to engage in additional profiling.[153] Pre-contractual and contractual measures are therefore unlikely to be a reasonable justification for online price-discrimination, and e-commerce providers will thus be likely to be required to acquire customer consent with the consequences described above.

Legitimate interests of the controller or a third party are a final possibility to process user data under the GDPR lawfully. In Recital 47, the regulation affirms that such legitimate interests can, for instance, occur when the data subject is a "client or in the service of the controller", however, the fundamental rights and legitimate interests of the data subject shall not be overridden, in particular in cases where the individual cannot reasonably expect further processing of their personal data.[154] While theoretically the controller could claim a legitimate interest in processing as part of his/her fundamental right to maintain a business, it has been argued that the two-tailed test that would determine whether this interest would override the fundamental rights of the data subject would be hard to fulfil in the case of online price discrimination, especially when there is a lack of transparency.[155] Of special importance in this regard is the judgement of the CJEU in the case of Google Spain v Española de Protección de Datos, in which the court held that economic interests of a controller cannot serve as a sufficient justification of legitimate interest alone, and would need to be accompanied by other balancing factors

[151] General Data Protection Regulation, *op cit.,* Art. 6 (1 b).
[152] Steppe, *op cit.*, p. 779.
[153] *Ibid.*
[154] General Data Protection Regulation, *op cit.,*Recital 47, Art. 6 (1 f).
[155] See in this regard the analysis of Steppe, *op cit.*, p. 780.

to allow the override of data subjects fundamental rights and interests.[156] Thus, legitimate interests would likely only possible to be invoked in combination with one of the other principles of lawfulness.[157]

5.2.2. Processing of Special Categories of Personal Data

For the subset of personal data that reveals the "racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation"[158] some additional, very strict requirements in terms of processing apply. In general, the processing of such data is prohibited, except in several instances of which the most important ones are cases where the data subject has provided explicit consent for one or more specified purposes or where the data subject has made the data manifestly public.[159]

In contrast to regular consent, which has already been severely strengthened compared to the standard of Directive 95/46/EC, explicit consent requires an 'express statement' of the data subject.[160] This higher standard can be fulfilled by obtaining a written and potentially signed statement (either on paper or uploaded to the internet) or by obtaining a confirmation via e-mail or the filling in of an electronic form.[161] In the case of data that has been "manifestly made public", it is not yet clear to what extent this will allow for a consent-free collection of special categories of data. It is likely that by this provision, data that a data subject shares freely available about him/herself without restricting the statement to a target audience will constitute a 'clear and affirmative action' that validates processing, e.g. when a person shares a clear affirmative statement of being a member of a certain ethnic or political group on social media (without having the statement limited to a group or audience such as family or friends).[162] This could, in theory, allow the acquisition of special categories of data through techniques such as web-scraping[163], but

---

[156] CJEU, *C-131/12 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, 2014, para 81.
[157] General Data Protection Regulation, *op cit.*, Art. 6 (1).
[158] *Ibid.*, Art. 9 (1).
[159] *Ibid.*, Art. 9 (2 a, e).
[160] Article 29 Working Party (GDPR Guidelines on consent), *op cit.*, p. 18.
[161] *Ibid.*
[162] Maria Roberta Perugini, *Personal Data made public by the Data Subject and use of Information on Social Networks.* Europrivacy, 2016, Available at: http://europrivacy.info/2016/10/31/personal-data-made-public-by-the-data-subject-and-use-of-information-published-on-social-networks-initial-observations-of-the-gdpr-art-9-para-2-letter-e-seco (consulted on 1.5.2018).
[163] Webscraping or Web data extraction refers to the practice of harvesting specified data bits on the internet through the application of software that mimics human browsing behaviour. Cf. Techopedia, *What is Web*

it is unlikely that the processing of data acquired in such a context would be beneficial for price-discriminating purposes since a processing of such data would still need to be conducted based one of the grounds for lawful processing such as consent or legitimate interest.

While the provision theoretically creates additional barriers to price discrimination based on criteria such as ethnicity or gender, direct discrimination based on the explicitly provided special categories of data would be unethical and possibly illegal anyways. In Recital 71 (2), the GDPR states explicitly that discriminatory effects based on the processing of special categories of data shall be prevented.[164] However, the mere omission of such data might still not rule out a pricing discrimination based on the traits protected by Article 9. Taken in isolation, the provision on special categories data only satisfies the 'minimal requirement' for non-discrimination; the listed categories are subject to special treatment. However, this does not capture the predictions made by algorithms based on proxy variables, which may target people from a certain group with the same accuracy as the special categories of data.[165] In fact when it comes to differential pricing, those categories may in some instances be among the most profitable options for segmentation, as big data allows detailed insights into behavioural patterns of genders and ethnic groups and in this way "digitally transmutes cultural clichés and stereotypes into empirically verifiable datasets", essentially blurring the line between value-added personalisation and harmful discrimination.[166] While dropping the sensitive criteria seems ineffective already, some argue that it may even be potentially harmful: If the special categories of data are not present in the dataset, it is not possible to check the correlation that other non-specified data points might have with those categories.[167] The 'maximum criterion' for non-discrimination of requiring data-sets to be corrected for potentially discriminatory proxy variables, already very hard or potentially impossible to be achieved, becomes thus even more complicated to address. Ultimately, the GDPR does therefore not offer a legal solution to the danger of proxy discrimination in pricing decisions, which may be anyway undesirable since the discussion on where to draw the line in this regard is far from being finished in computer science and philosophy alike. A

Scraping? Available at: https://www.techopedia.com/definition/5212/web-scraping (consulted on 5.1.2018).

[164] General Data Protection Regulation, *op cit.*, Recital 71 (2).

[165] Bryce W. Goodman, 'A Step Towards Accountable Algorithms?: Algorithmic Discrimination and the European Union General Data Protection', in: *29th Conference on Neural Information Processing Systems*, Barcelona, 2016, p. 3.

[166] Schrage, *op cit.*

[167] Goodman, *op. cit.*, p. 4.

mitigation of proxy discrimination may, however, be derived from the GDPR provisions related to profiling and transparency, which will be explored in Sections 5.3.1 and 5.3.4.

5.3. Rights of the Data Subject

The GDPR strengthens the rights of the data subject and, in several cases, confers new ones to it. Some of those rights will have a notable impact on the way data processing can be conducted, which will in turn also have an influence on the price discrimination techniques that could be potentially carried out through such practices. This section evaluates the potential impact of the rights of the data subject regarding transparency, information and access, rectification and erasure and automated individual decision-making.

5.3.1. Transparency and Information Access

The GDPR aims at reducing information asymmetry by giving data subjects an extensive amount of information at the point of collection (or within a reasonable time period in cases where the data has been acquired by a third party).[168] The information that should be provided includes formalities such as the identity and the contact details of the controller and the legal grounds for and purposes of the processing, but also information on the storage periods, on whether the data is intended to be transferred to third countries and whether the data is used in the process of automated decision making or profiling.[169] This refers not only to instances in which an individual consciously provides its personal information to a controller (e.g. through an electronic form) but also to the case that a controller obtains information on the individual through observation or tracking technologies.[170] Consequentially, the provision essentially covers all possibilities for tracking consumers through the technologies outlined in Chapter 4.1.1., and therefore severely reduces the opacity of such processes. Overall, the GDPR requires controllers to use clear language that avoids both complex and long sentences and language qualifiers such as 'may', 'might' etc., and the information needs to be placed at a location that does not require search efforts for consumers.[171] Although it remains to be seen to what extent controllers will actually refrain from using "overly legalistic, technical or specialist language or terminology"[172], the regulation delivers a new benchmark in transparency

[168] General Data Protection Regulation, *op cit.*, Recital 61.
[169] *Ibid.*, Art. 12 (1) in conjunction with Art. 13 (1, 2) and Art. 14 (1, 2), Recital 60.
[170] Article 29 Working Party (Guidelines on Transparency), *op cit.*, pp. 14-15.
[171] *Ibid.* pp. 8 – 10.
[172] *Ibid.*, p. 10.

that could finally give consumers what many privacy economists long demanded them to have: a higher degree of bargaining power in their transactions with the processors of their personal data.

In the context of big data analytics, however, it is noteworthy that transparency may become difficult to implement and thus to enforce. Where automated decision-making or profiling is involved, there should be "meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject".[173] In combination with Recital 71 which envisions that individuals should be able "to obtain an explanation of the decision reached"[174], these provisions have sparked a heated debate among scholars whether the GDPR establishes a 'right to an explanation of an automated decision'. While some argue that there is no legal obligation to truly explain algorithmic decisions under the GDPR *ex-ante* or *ex-post* to a decision,[175] others hold that Articles 13, 14 and 15 do in fact provide a right to be informed about the functional making of the decision.[176] Whether and how an explanation could actually be invoked remains to be seen after the entry into force of the GDPR, but the guidelines of the Article 29 Working Party suggest that an overly detailed insight into the decision-making process may not be necessary. According to the working party's document, explaining the data subject in simple terms the rationale behind a decision and/or the criteria for the decision would suffice, including for instance an explanation why the algorithm is used and disclosing the information the processor held about the individual.[177] Consequently, it can be argued that it is unlikely that data subjects will be able to demand extensive insight into the mechanics that led to the display of a particular price to them. The disclosure of the related information may, however, give them enhanced chances to alter their profiles to conduct arbitrage.

When the obtained data is determined to be further processed in big data analytics, the information provided should also involve the "intended purpose of creating and further processing such inferred personal data, as well as the categories of the inferred data processed".[178] As discussed before, the latter provision might still not be up to the task of

---

[173] General Data Protection Regulation, *op cit.*, Art. 22 (2 f)
[174] *Ibid.*, Recital 71 (1).
[175] Sandra Wachter, Brent Mittelstadt and Luciano Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation', in: *International Data Privacy Law*, 2017, pp. 7-19.
[176] Andrew D. Selbst and Julia Powles, 'Meaningful information and the right to explanation', in: *International Data Privacy Law*, Vol.7, No.4, 2017, p. 242.
[177] Article 29 Working Party (Guidelines on profiling), *op cit.*, p. 14.
[178] Article 29 Working Party (Guidelines on Transparency), *op cit.*

fully informing individuals about the ways in which artificial intelligence can deduct information on them, but it is certainly a good starting point. As elaborated in the previous section on consent, the extent to which consumers would agree or object to such additional inference creation might ultimately also depend on the way the price discrimination is framed by the supplier. Because the categories of inferred data will need to be indicated, the transparency provisions could further unfold a mitigating effect on proxy discrimination, since it would result in a situation in which consumers would need to consent to be price discriminated based on their (inferred) ethnicity or gender. On the other hand, the 'black box' of algorithms can lead to suppliers not knowing themselves which categories are inferred,[179] thus making full transparency in this regard a difficult provision to fulfil.

Regarding big data analytics facilitated 'nudges', it has already been argued in section 5.2.1. that the difficulty of attributing a specific purpose to a given (personalised) choice architecture makes it unlikely that the GDPR will influence such practices. The same can be held regarding the right to information: Even if the rather dark scenario developed by some scholars regarding a situation in which firms increasingly "morph" their websites to capitalise on certain predicted customer weaknesses (e.g. self-esteem) was to materialise,[180] the explanation of the "logic involved" as demanded by the GDPR can be regarded to go not as deep as to require the uncovering of such underlying motives. Because the primary function of the adaptation would, after all, be a personalisation of the website, suppliers would thus also only need to inform their customers about that logic – without pointing out the potential nudge.

5.3.2. Rectification and Erasure

Data subjects have the right to request access to the information about data that is processed in regard to them (cf. section above) within one month and shall have the right to rectify any data that is incorrect.[181] While those rights do not pose a substantial change to the previous standard of Directive 95/46/EC and are not particularly relevant to online price discrimination,[182] the rights to restriction of processing and the right to erasure (also

[179] Goodman, *op. cit.*, pp. 3 – 4.
[180] Cf. Calo, *op cit.*, p. 1018.
[181] General Data Protection Regulation, *op cit.*, Art. 15, 16.
[182] Steppe, *op cit.*, p. 782 concludes that while the right to rectification gives data subjects a possibility to correct 'false positives' based on which they may be discriminated, the effect of the right is marginal because data subjects rarely know if and how they are segmented and that price discrimination can still occur perfectly based on the rectified data.

called the 'right to be forgotten') have attracted the interest of scholars in regard to big data contexts.

The right to be forgotten as specified in the GDPR can, although in general present in scholarly thought since the 1990's, be regarded as an enshrining of the controversial judgement in C-131/12 *Google Spain SL, Google Inc.* v *Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, in which the court recognised such a right in cases where data is "inadequate, irrelevant or excessive in relation to the purposes of the processing", even if the data had been hitherto processed lawfully.[183] In the GDPR legal context, data subjects can request the erasure of their data in a variety of cases, e.g. where they withdraw a previously given consent, object to an automated decision or when the processing has generally been unlawful or has lost its original purpose.[184] The new provision differs from the CJEU judgement and the respective Article 29 Working Party guidelines to the extent that the ruling applied to an intermediary controller of personal data (in that case Google Spain), while the regulation serves as a basis to request erasure from any controller.

Scholars have recently pointed out that while the GDPR does not clarify what exactly is meant by "erasure" in data processing terms, but that a strict interpretation as a full deletion of the data in a database could potentially endanger the consistency of databases and might even lead to their break-down.[185] The problem relates to the internal functioning of real time-databases, where the processes of atomicity, consistency, isolation and durability (ACID) often require the information to exist at multiple places in the database at the same time, as well as in several logs and backup files. Normally, data that is requested to be deleted is excluded and detached from future search queries in the database but remains intact until it is overwritten by new information, which can often take extended periods of time.[186] If this process is required to be substituted through an immediate deletion or anonymisation, it produces severe efficiency reductions for artificial intelligence.[187] The issue highlights general misalignments that can occur when technical realities are not taken into due considerations by regulators. If strict deletion would be enforced after the entry of the GDPR, online price discrimination could face severe problems: If a sufficient amount of people would, in line with the regulation,

[183] C-131/12, *op cit.* para. 92 – 96.
[184] General Data Protection Regulation, *op cit.*, Art. 17 (1), Recitals 65, 66.
[185] Eduard Fosch Villaronga, Peter Kieseberg and Tiffany Li, 'Humans forget, machines remember: Artificial intelligence and the Right to Be Forgotten', in: *Computer Law & Security Review*, Vol.34, No.2, 2018, p. 309.
[186] *Ibid.*
[187] *Ibid.*, p. 310.

request the erasure of their data (e.g. through withdrawing their consent), the price discriminating algorithms could effectively lose their capacity to efficiently segment the users because their underlying models would be distorted. Since the interpretation of erasure is however not yet clear, it can, however, be argued that the enforcement of the GDPR is unlikely to adopt an overly orthodox approach to erasure, especially considering that it would result in disastrous detriments for all AI industries which can be subject to data subjects' erasure claims. It is, for instance, possible that in cases where a request for erasure meets artificial intelligence processing, the two-tailed balancing test regarding the legitimate interests of controller and data subject would favour the former: While the data subject's legitimate interest is satisfied through the exclusion of his/her data from the search queries of the database and thus from direct outputs regarding him/her, the controller can keep the data with the legitimate interest of the functioning of his application, even if the ultimate erasure (or more adequately: override) of the personal data would ultimately take more than one month. This would effectively resemble a temporary restriction of processing as specified in Article 18 GDPR[188] until an override can take place. Regardless of how the right to be forgotten is going to be interpreted, its implementation will definitely require adjustments in the algorithms used for online price discrimination. While some similar technical adjustment necessities (e.g. the requirement to make the new types of data covered by the regulation legally compliant) have been introduced in this research before already, this can be seen as the most important example of a way in which the GDPR can have a *direct impact on the technical implementation of online price discrimination*.

On a behavioural note, some authors have also argued that the existence of a right to be forgotten would enable individuals to freely express themselves because they would no longer have to fear that their current actions would haunt them indefinitely in the future. [189] Empirical evidence indicates that the existence of such a right can correspondingly also positively influence the privacy calculus of individuals, resulting in a higher willingness to provide their data.[190] Further empirical evidence will be necessary after the entry into force of the GDPR, especially in regard to highly sensitive issues such

[188] General Data Protection Regulation, *op cit.*, Art. 18
[189] Bert-Jaap Koops, 'Forgetting Footprints, Shunning Shadows: A Critical Analysis of the 'Right to Be Forgotten' in Big Data Practice', in: *Tilburg Law School Research Paper No. 08/2012*, Vol.8, No.3, 2012, pp. 24-25.
[190] Nigel Mangwanda, *The impact of the right to be forgotten on privacy and online information disclosure*. University of Pretoria, Johannesburg, 2016, p.81.

as pricing, but it appears that there is a potential for a positive (interfering) effect of the right to erasure on the decision to consent to the processing of personal data.

5.3.3. The Right to Data Portability

Data subjects have the right to obtain personal data they have wilfully provided or that was automatically processed in a machine-readable format that can be taken to an alternate controller without restrictions by the controller the data was originally provided to.[191] The right establishes a further balancing in the power-relationship between controller and data subjects, as the latter can now in principle freely choose to provide his/her data to a controller they like better, leading to potentially higher competitive pressures.[192] Interestingly, the right distinguishes between personal data that was "provided by the data subject", which includes data that was observed concerning the behaviour of an individual on a website and data that is inferred based on such provided data. The latter, containing for instance data created in the process of profiling and user segmentation, is not affected by the right to data portability and remains with the controller who inferred the data.[193]

For online price discrimination, this means that data subjects can transport the data that constitutes the basis for categorisation and subsequently price discrimination from one controller to another, but their full (inferred profile) will not switch. While users who benefitted from price discrimination on one website could thus not expect the same benefits to occur automatically in another shop, the distinction introduces an element of comparability: It is conceivable that consumers could provide the same dataset to multiple suppliers to see where they get the best offer. This could, in theory, lead to the paradoxical situation that consumers who benefit from price discrimination would choose the supplier with the best segmentation system, while those who would pay higher prices would choose the supplier with the worst (or non-existing) segmentation algorithm. Overall, if such a fluid comparison was actually to emerge, it could become difficult for suppliers to charge users a price for a good that is significantly higher than its general market price.

Data portability may also stimulate price discrimination as a churn prevention effort (c.f Chapter 3.2.): services offered to users that are primarily based on provided user data

---

[191] General Data Protection Regulation, *op cit.*, Art. 20 (1 a, b).
[192] Consider that the Working Party's interpretation of the right as "enhancing individual's control over their personal data and making sure they play an active role in the data ecosystem" and the acknowledgement that this can lead to competitive pressures: Article 29 Working Party, *Guidelines on the right to "data portability"*, Brussels, 2017, p. 4.
[193] *Ibid.*, pp. 9-10.

(e.g. social platforms or dating websites) could be incentivised to counter the increased ease of customer churn by giving their existing users additional benefits, including preferential prices. Not only churn prevention offers are potentially costly, but also the compliance with the right to data portability as such, which could thus become a market entry barrier and innovation impediment.[194] These concerns are based however on the assumption that the right is expensive to implement; if this is not the case economic analysis predicts the opposite effect and assumes both a reduction of market entry barriers and an incentive to innovate.[195] The economic argument introduced in section 3.2. that information sharing between price discriminating companies is always beneficial for their profit maximisation should also be kept in mind here. Whether companies with innovative pricing strategies will benefit or suffer from data portability will therefore ultimately depend on how fast a common standard for the data export is found and how expensive it will be to implement.

Finally, the right to data portability could also lead to more comprehensive user profiles: The possibility to extract and combine one's personal data from multiple services could result in a 'fusing scenario' which would "turn the fragmented multiplicity of digital services into interoperable segments of a user-centric Internet of things".[196] Regardless of which competition effects portability will entail, user profiles could indeed become increasingly detailed through combination and would thus increase the accuracy of customer segmentation algorithms overall. Although formally a processor that is entrusted with data taken from another controller is not allowed to make excessive use of such data (i.e. using it for another purpose than the one it is provided for),[197] it is still conceivable that more in-depth profiling will be possible in all cases in which data subjects (i) explicitly provide their profile to receive targeted price offers or (ii) consent to receive such offers in the environment of the new controller.

---

[194] Inge Graef, Jeroen Verschakelen and Peggy Valcke, 'Putting the Right to Data Portability into a Competition Law Perspective', in: *The Journal of the Higher School of Economics Annual Review*, 2013, p. 62.
[195] Michael Wohlfarth, 'Data Portability on the Internet: An Economic Analysis', in: *28th European Regional Conference of the International Telecommunications Society (ITS): "Competition and Regulation in the Information Age"*, Passau, 2017, p. 17.
[196] Paul De Hert, Vagelis Papakonstantinou, Gianclaudio Malgieri, Laurent Beslay and Ignacio Sanchez, 'The right to data portability in the GDPR: Towards user-centric interoperability of digital services', in: *Computer Law & Security Review*, Vol.34, No.2, 2018, p. 202.
[197] Article 29 Working Party (Guidelines on portability), *op cit.*, pp. 6-7.

5.3.4. Right to Object and Automated Individual Decision-Making

Data subjects have the right to object to processing carried out based on the legitimate interests of the controller,[198] which is essentially a balancing provision to the lawfulness processing-ground of legitimate interest as discussed in Chapter 5.2.1.

More interesting in regard to online price discrimination is the right "not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her".[199] As noted by Steppe, the application of the provision to price discrimination is somewhat troublesome.[200] The first criterion, 'based solely on automatic processing', which the Article 29 Working party considers as "no human involvement in the decision process"[201], is easily satisfied by customer segmentation through big data analytics. Regarding the producing of legal effects, it is necessary that the processing has an impact on an individual's legal rights, alters its legal status or its rights under a contract.[202] This can be argued to be the case when an individual completes a purchase on a website, and possibly even to the setting of the price prior to the purchase: an individual could be argued to have the right to accept a proposal for certain goods and services, the offer thus having legal effect.[203] Furthermore, the formulation "significantly affects him or her" could be applied to price discrimination, since a price that varies largely could have a considerable impact on the data subject (arguably depending on *how much* the price varies).[204]

Since the legal status of an indirect 'right not to be subject to price discrimination' is already ambiguous, it is difficult to assess how it would translate into practice. Firstly, is important that the right will not apply in cases where the automated processing is necessary for the performance of a contract or where the data subject has given his/her explicit consent.[205] Since online price discrimination will likely have to rely on consent, the full right to object automated decisions based on the data provided this way will correspondingly not apply. Nevertheless, Article 22 (3) still establishes the right to at least "obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision"[206]. This implies a review of the decision by a natural

[198] General Data Protection Regulation, *op cit.,* Art. 21 (1).
[199] *Ibid.,* Art. 22 (1).
[200] See the analysis of Steppe, *op cit.*, p. 10.
[201] Article 29 Working Party (Guidelines on profiling), *op cit.*, p. 9.
[202] *Ibid.*, p. 10.
[203] Steppe, *op cit.*, p. 10.
[204] Cf. *Ibid.*
[205] General Data Protection Regulation, *op cit.,* Art. 22 (2 a, c).
[206] *Ibid.*, Art. 22 (3).

person with authority to revoke the decision, based on a detailed review of the data used in the decision-making process as well as possible additional data provided by the data subject.[207] The challenge thus ultimately lies again in making the decision-making process of artificial intelligence comprehensible for humans; a controller would need to be able to understand why his system arrived at a particular outcome. For artificial intelligence, there is the additional problem that even if the steps of the decision can be re-enacted, a full comprehension would still not be possible unless the training component through which the algorithm originally learned its structuring approach is provided as well.[208]

5.4. Case Study: Price Personalisation based on Geographic IP Data

In the following, the case of a company that offers geographical price personalisation based on artificial intelligence is used as a practical example for the implications of the GDPR for price personalising businesses.

Darwin Pricing was established recently in July 2016. It provides a machine learning solution that can be implemented in a customer company's pricing system and learns autonomously based on the acquired data.[209] The pricing system works through assessing a customer's geolocation through his/her IP-Address and learning regional patterns based on A/B testing, i.e. a testing phase in which the price performance in different geographical regions is evaluated. Once a price level has been established, the algorithm can provide either geographically customised prices or display geographically customised discounts for the customer company's webshop's uniform price.[210] The algorithm also reacts to demand fluctuations and competitor prices by continuously reassessing the success of the estimated willingness to pay rates and adjusting the respective discounts accordingly. To prevent potentially negative reactions from customers to a price change, the price for a given customer remains the same for his/her IP-Address.[211] Finally, behavioural data of website visitors is also assessed (such as scrolling, length of stay on the website or mouse movements), which are used to determine the point in time of the

[207] Article 29 Working Party (Guidelines on profiling), *op cit.*, p. 15.
[208] Sven Jacobs and Christoph Ritzer, *Data privacy: AI and the GDPR.* Norton Rose Fulbright, 2017, Available at: https://aitech.law/blog/data-privacy-ai-and-the-gdpr (consulted on 6.5.2018).
[209] Darwin Pricing Survey Results (Annex 1), received on 25.4.2018, p.10.
[210] Darwin Geo-Pricing, *Price for Profit with the World's Leading Dynamic Pricing Solution For Geo-Targeted Price Optimization.* Available at: https://www.darwinpricing.com/de/ (consulted on 7.5.2018).
[211] *Ibid.*

discount offer.[212] Although Darwin Pricing does not engage in the type of first-degree price discrimination based on extensive profiling that can be expected to be the most affected by the GDPR, the case certainly allows for a beneficial testing and exploration of the insights gathered in the previous sections.

While the behavioural data of the customers are processed only by the browser of the respective user and not the pricing algorithm itself, thus not falling under the regulation's material scope, IP-Addresses will be considered personal data under the GDPR and will thus be subject to the provisions outlined in Chapter 5. Darwin Pricing does, however, offer its customer companies a tool for anonymisation of the acquired IP-Addresses.[213] In cases where such software is used, the processing of the IP addresses would thus not fall under the material scope of the GDPR any longer.[214] Nevertheless, all customer companies who will continue to work with non-anonymised IP-Addresses in the EU will need to establish informed consent. Customers who visit an e-commerce website that implements the indicated pricing solution will thus need to consent to receive personalised price offers. According to Article 13 (f) and 14 (g) GDPR, the consent procedure would need to involve the providing of information about (i) the fact that automated decision making is going to occur, (ii) the logic involved in assessing the geographical region's price elasticity and (iii) that, as a consequence of the processing, the user can, but not necessarily will, get a price discount. Darwin Pricing correspondingly expects a reduction of the data that will be available to the data economy, since profiling based on browsing behaviour will not be allowed anymore without explicit consent.[215] In the given business model, a denial of the customer to have his IP address processed with the purpose to receive personalised price offers would, in the end, result in getting displayed a uniform price, which would result in a reduction of his/her welfare because the discounts offered are per definition below the uniform price. Regarding the danger of proxy discrimination, the geo-targeting can locate the anonymised IP-Addresses with about 30 kilometres accuracy,[216] which can be seen as a very low risk concerning the issue of accidentally targeting specific ethnicities. A right not to be subject to an automated decision would likely not apply in the decision-making process of Darwin Pricing's algorithm because an explicitly provided consent would reduce the right to the proceedings of Article 22 (3) GDPR. While data subjects could still demand human

[212] Sébastien Fauvel, Written communication of the general manager of Darwin Geo-Pricing (Annex 2), received on 7.5.2018.
[213] *Ibid.*.
[214] See General Data Protection Regulation, *op cit.*, Recital 26.
[215] Darwin Pricing Survey Results, *op cit.*, p. 15.
[216] Fauvel, Written communication, *op cit.*

interaction and a review of the decision pursuant to Article 22 (3) GDPR, the human review would likely be satisfied by confirming that the IP address of the user corresponds to the region to which a certain coupon applies. A change of the decision could only be invoked if the data subject would provide additional information that indicates his/her residence in a region that is affected by a different coupon. Ultimately, the high effort that this procedure requires from the customer makes it counter-intuitive that the right would actually be invoked. Interestingly, the biggest challenge identified by the company regarding the GDPR's application to artificial intelligence refers to the issue outlined in chapter 5.3.2., scilicet the right to erasure. In this regard, it indicated that "making user data deletable requires some adjustments in internal processes".[217] Taking into account that the attribution of user's IP-Addresses to geographical regions form part of the training process of the pricing algorithm and considering the technical reality of timely deletion of data in large databases in general, the implementation of Article 17 GDPR can indeed be considered difficult, however the pricing company indicated that it is possible to meet the standards. Firstly, where anonymised IP-Addresses are used, the right to be forgotten does not apply because the users are not identifiable in the first place. But even in cases where customer companies do continue to work with identifiable IP-Addresses, deletion is possible within one month because the applied machine learning solution is regularly retrained. Thus the autonomous learning capabilities of the algorithm enable a timely substitution of the customer data that is requested to be deleted.[218]

Despite the identified issues of a likely reduction of the available personal data and the challenge of deletion, the company is optimistic that privacy legislation will ultimately lead to higher trust and better acceptance of e-commerce in the market, accelerating the growth of the industry.[219] The example of the examined pricing company underlines that privacy enhancing technologies (cf. Chapter 4.1.2.) can be a key tool to make price-personalisation approaches GDPR-compliant. Additionally, the example highlights how certain behavioural categories can be used for price personalisation without requiring them to be processed as personal data: In the present case, data such as scrolling behaviour is used to trigger the point in time a discount offer occurs. Because it is only processed by the user's browser, the monitoring does not create personal data but nevertheless fulfils a potential pricing function: Users with a higher willingness to pay might proceed faster to a purchase and thus indirectly self-select themselves to pay a higher price, while customers whose browsing of the website indicates a lower willingness to pay (e.g. long

[217] Darwin Pricing Survey Results, *op cit.*, p. 16.
[218] Fauvel, Written communication, *op cit.*
[219] Darwin Pricing Survey Results, *op cit.*, p. 15.

periods of inactivity that may correspond with the checking competitors' websites) will eventually get displayed a regional discount. In general, the latter selection mechanism is rather indirect, and the relationship with the customer's willingness to pay is arguably ambiguous. The feature may thus be understood better as a soft form of 'nudging' the customer by influencing his/her purchasing decision at the right point in time when it does not disturb the user experience. Nevertheless, the two-stage process ultimately entails two rough types of customer segmentation, firstly according to their geographical area and secondly according to their willingness to pay as estimated from their conversion rate. The technology can subsequently yield significant profit increases.[220]

To conclude, the given example implies that there are models of consumer segmentation that are only marginally affected by the GDPR.[221] From an economic perspective, the low interference of the GDPR with geographic price discrimination can however be considered as desirable, as a situation in which the inability to lower prices in areas with a lower intensity of demand would likely result in a discontinuing (or non-entry) of a supplier in the respective regional market, leading to a loss in welfare that is undesirable from a regulatory point of view.[222] In the case of Darwin Pricing, a consumer surplus extraction only occurs for those customers who pay the uniform, undiscounted price, while the willingness to pay adaptation for the discounted customers does not go beyond adjusting the price to the regional average willingness to pay. In such a case, the non-interference of the GDPR can thus be considered to sustain market opening capacities.

5.5. Integration of Insights

Following the detailed review of the relevant provisions of the GDPR under consideration of the implications of price discrimination theory and big data analytics, some general conclusions on the impact of the regulation on online price discrimination can be drawn. There are generally three types of impacts stemming from the GDPR that should be anticipated. The first one, a *direct impact on the technical implementation of online price discrimination*, does not substantially differ from the general implications of the

[220] Darwin Pricing, *Case Study: Worldwide Cyclery.* Available at: https://www.darwinpricing.com/sales/brochures/case-studies/worldwide-cyclery/en/Case_Study_Worldwide_Cyclery.pdf (consulted on 8.5.2018).
[221] Note that this corresponds with the prediction that the GDPR would not extensively apply to price discrimination based on single, rather rough criteria stated in section 5.1.
[222] Cf. Damien Geradin and Nicolas Petit, 'Price discrimination under EC competition law: Another antitrust doctrine in search of limiting principles?', in: *Journal of Competition Law & Economics,* Vol.2, No.3, 2006, p. 485.

regulation for companies who engage in the processing of personal data through big data analytics. As for many industries who use personal data to train artificial intelligence, the right to be forgotten, the right to object to an automated decision, the right to data portability and the right to explanation (as far as it will be applied in practice) can pose a challenge to online price discrimination in regard to the extent that gathered user data can be deleted without detriments to the algorithm and the extent to which the calculated decisions can be explained. Regarding the latter, the judicial interpretation of the 'right to explanation' will determine the extent to which extensive algorithmic transparency will actually be required, and thus whether it actually counts as a direct impact on technical implementation. The material scope of the regulation is another vital factor in regard to technical implementation, as it is going to capture virtually all of the types of data that can be used for online price discrimination and will thus render the majority of companies conducting such practices subjects to the GDPR's technical implications. While the example of the examined company Darwin Pricing shows that in the case of regionally applied third degree price customisation, privacy-enhancing technologies such as anonymisation can be applied easily to remove the approach from the scope of the GDPR, such a model would not be possible to use for a company that implements a first-degree price discrimination approach.

The second type of impact can be characterised as a *behavioural empowerment impact on the technical implementation of price discrimination* and is closely related to the first type of impact, but in addition depends crucially on the extent to which users will make use of the rights conferred to them under the regulation. This entails most importantly the factor of informed consent, but to a lower extent also the right to data portability. In the first case, the extent to which customers make use of their right to opt out from price personalisation following the request for informed consent will determine the amount of customer data that is available to the computing of willingness to pay and the number of customers that can be provided with personal offers in the first place. This could, in theory, lead to a reduction of the accuracy of price-personalisation algorithms. However, the review of the functioning of big data analysis in Chapter 4 suggests that as long as a valid training set is available, the output-accuracy should be possible to be maintained. The right to data portability could, in turn, depending on the extent to which consumers (i) combine their data of multiple digital profiles and (ii) provide consent to a new controller to process those profiles, lead to an increase of customer data for price-discrimination purposes and thus to an increase in targeting accuracy. The welfare implications of a more efficient consumer segmentation in online environments appear ambiguous: While there is little evidence available on the welfare implications of a first-degree segmented distribution of physical goods, a less efficient targeting might be detrimental to the welfare of both suppliers and consumers in regard to digital goods (cf. section 3.2).

Equally, the question whether customers will provide their consent uniformly among companies or, as some evidence suggests (cf. section 5.2.1), prefer bigger companies they are familiar with also has potential welfare implications regarding competition.

Finally, there is a *behavioural empowerment impact on societal welfare*. First and foremost, the combination of material scope, the right of information and the requirement of informed consent suggests that all types of first-degree price discrimination will need to be actively opted in by consumers, which results in a significantly enhanced degree of choice and thus a serious decrease of the informational asymmetries that were hitherto assumed in the digital privacy literature. While this is a positive welfare effect as such already, the economic impact of the empowerment of choice remains ultimately ambiguous, as empirical evidence on how consumers will make use of consent is yet to be obtained. Using insights from behavioural economics, it was argued that the success of obtaining consent to price-discrimination might heavily depend on the framing of the price discrimination and that consumer opt-in is likely to be higher in cases where preferential offers or discounts are promised. In such cases, the welfare effect would mirror the model of mutually beneficial price-discrimination that was proposed for digital goods in Chapter 3.2., as no customer would pay a price higher than the uniform one.

Next to the potential effects of the GDPR outlined above, it is also noteworthy what is *not* going to be affected by the regulation, most importantly the issue of proxy discrimination. As argued before, the strict handling of special categories of data could in fact lead to the perverse effect that price discrimination based on sensitive criteria is going to increase rather than decrease because in cases where the explicit criteria such as ethnicity or gender are not obtained by a controller, the pricing algorithms cannot be trained to omit other data types that correspond to the special categories. Another feature that is relevant to online price discrimination but that is unlikely to be captured by the GDPR is the practice of nudge. Although the choice environment of a website can be considered to be highly relevant to the purchasing decision of a customer or his/her provision of consent, the creation of such adjustable features does not rely on personal data to an extent that would require informing the customer or to seek his confirmation. As shown in the example of Darwin Pricing, it is possible to address customers based on behavioural data that is solely processed by the user browser, enabling a form of anonymous personalisation that is not captured by the GDPR.

To summarise; the proposed impact categories are not mutually exclusive and since the different provisions of the GDPR are heavily interdependent, so are the types of impact anticipated by this research. Table 1 gives an overview of the findings of the analysis and the respective inferences drawn in this section. Note that findings regarding

ambiguities in the legal interpretation or non-application of the regulation are largely omitted from the overview.

GDPR Provisions	*Direct impact on the technical implementation of online price discrimination*	*Behavioural impact on the technical implementation of price discrimination*	*Behavioural Impact on Societal Welfare*
Material Scope of Application: Art. 4, Recitals 26,	Wider scope of data affected; low thresholds of identifiability	Wider use of consent necessary (cf. below)	N/A
Consent Procedure: Art. 4 (11), 7, Recitals 32, 42, 43	Overall fewer consumer data available	Users unlikely to opt-in to price-discrimination; potential reduction in user data Users potentially more likely to opt-in to provide their data for discount offers; potential steadiness/increase in user data	Potential Competition Detriments; market barrier entries for new companies who may not obtain consent Increase/Decrease in Consumer Surplus Extraction depending on customer data provision choices
Special Categories of Data: Art. 9, Recital 71	Potentially higher degree of discrimination based on inferred sensitive data because models cannot be corrected	Explicit consent needed from data subject to allow processing.	(No rectification of potential socially undesirable dis-crimination effects)
Transparency: Art. 12, 13, 14, 15, Recital 61	Possible right to explanation: Requirement to construct algorithms in a way that allows for a detailed review of the decision-making process (cf. right not to be subject to an automated decision)	Necessity to inform customers about the types of data collected and the purpose of price personalisation for the processing	Reduced Information Asymmetry in Data/Service Trade-Offs
Right to Rectification: Art. 16	Provision of rectification possibilities in price discriminating algorithms necessary	Correction of 'false positives' leads to more accurate consumer targeting	Possible replacement of consumers in another pricing segment with the corresponding surplus effects
Right to Erasure: Art. 17, Recitals 65, 66	Severe efficiency impediments if interpreted strictly as an immediate deletion even in big data analytics	Potentially higher willingness to disclose data among data subjects in the presence of an RTBF	N/A
Right to Data Portability: Art. 20, Recital 68	Necessity of interoperability of customer data	Easier acquisition of more extensive user profiles, more effective customer segmentation (dependent on consent)	Depending on provision of consent to new market players: either enhanced competition (if high) or barriers to market entry (if low)
Right not to be subject to an automated decision: Art. 22, Recital 71	Potential need to make algorithms comprehensible for humans (however unlikely)	N/A	Potential (further) reduction of information asymmetries

Table 1

6. Discussion and Conclusion

This study applied an interdisciplinary approach to explore the potential impact of the General Data Protection Regulation on AI facilitated online price discrimination.

In an element of discussion, it has to be stated that a cross-matching of economic theory with insights from computer science and legal studies can in no way substitute the empirical research that is going to be necessary to test the assumptions and predictions that were achieved throughout the course of this research. Such empirical evidence will only be possible to be obtained in the medium term, after a reasonable amount of time following the entry into force of the regulation. The answer to the research question is thus but a framework for future research, as a definite answer to the effect of privacy regulation on online price discrimination is, as demonstrated in this study, dependent on a large number of variables that await confirmation or rejection. The uncertainties that remain not only for researchers but also price personalising businesses stem from various fields and depend on very different types of actors. To give an example, the question if and to what extent a company deploying a price discriminating algorithm actually needs to provide detailed insight into the working of the algorithm (including the decisional patterns it acquired in its training phase) can only be answered by a court in a final interpretation of the debate about a 'right to explanation'. If and how such a right would then be possible to be implemented in the context of big data analytics would, in turn, be a technical challenge, dependent on the development of new auditing techniques that are able to break open the black box of algorithms. In a similar fashion, the outcome of a variety of issues (such as the accuracy of price discrimination algorithms or the number of customers to which those algorithms apply) has been shown to be crucially dependent on the choices that customers are going to make regarding the provision of their consent in the future. A final issue that should be kept in mind is that this research focused on the impact of the GDPR on the practice and implementation of online price discrimination. Challenges such as transaction costs of the regulation for instance caused by increased bureaucratic burden should be considered in researches that focus on the impact of the regulation on the online price discrimination industry as a whole.

The considerations above underline that it lies in the nature of exploratory research to take all findings with a high degree of caution. Nevertheless, the research question was possible to be answered in a way that allows for some important predictions for the future of online price discrimination in the EU, as well as for the identification of issues for further research. As proposed earlier, the impact of the GDPR on online price discrimination can be considered to be three-fold: A direct impact on its technical implementation, a behavioural empowerment impact on its technical implementation and a behavioural empowerment impact on societal welfare. While the total welfare

implications are hard to estimate and depend on the industry in which the price discrimination is conducted, the method of price discrimination pursued and the behaviour of consumers, the overall empowerment of choice on the side of individuals overall hints at a reduction of the future capacity of online business to extract consumer surplus. To acquire a more detailed understanding of the regulation's impact, multiple empirical tests of the derived categories are necessary and should be considered in future research. Most importantly regarding the conditions under which consumers will provide their consent to personalised price offers, but also in regard to the potential challenges posed by the regulation to the further development of price personalising artificial intelligence. Furthermore, the landscape of online price discrimination in the EU needs to be better assessed, as this research suggests that the impact of the GDPR is heavily dependent on the type of price personalisation pursued. While types such as geographic price discrimination can be conducted with low privacy interference and might therefore only be marginally affected, the regulation's impact on practices that require a more in-depth knowledge of customer traits (for example churn prevention) can be expected to be more profound. Whether that is going to be beneficial or detrimental to consumer welfare remains to be seen and needs to be observed for a more extensive set of markets: In the examined case presented in this study, less privacy interference correlated with a welfare creating, market opening price discrimination approach, but that does not always have to be the case.

Under the reservation that several legal questions regarding the regulation's application still await their final confirmation, the intuitive consideration that the more privacy-invasive a certain price discrimination approach is, the more it is going to be affected by the GDPR generally seems to hold, not least due to the extensive scope of the legislation and its focus on consent and transparency. Although the GDPR gives little progress on some of the bigger ethical questions regarding the relationship between online price discrimination and big data analytics, scilicet the issues of proxy discrimination and the erosion of customer autonomy through nudge choice architectures, the general technological development towards the potential of first degree price discrimination is certainly going to be accompanied and influenced heavily by the EU's new rigid privacy regime – and thus not least by the deliberate choices of consumers.

Bibliography

A. Primary Sources

Documents

Darwin Pricing Survey Results (Annex 1), received on 25.4.2018.

FAUVEL, Sébastien, Written communication of the general manager of Darwin Geo-Pricing (Annex 2), received on 7.5.2018.

Legislation and Court Cases

CJEU, *C-582/14 Breyer v Bundesrepublik Deutschland*, 2016.

CJEU, *C-131/12 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, 2014.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

Statistics

Eurostat, *Privacy and protection of personal information* , Available at: http://appsso.eurostat.ec.europa.eu/nui/submitViewTableAction.do (consulted on 22.2.2018)

B. Secondary Sources

Books

CARLTON, Dennis W. & PERLOFF, Jeffrey M., *Modern Industrial Organization* (4th edition). Addison-Wesley, Boston, 2005, 822 p.

MANGWANDA, Nigel, *The impact of the right to be forgotten on privacy and online information disclosure*. University of Pretoria, Johannesburg, 2016, 128 p.

REPKO, Allen & SZOSTAK, Rick, *Interdisciplinary Research: Process and Theory* (3rd edition). Sage, Los Angeles, 2017, 425 p.

STIGLER, George J., *The theory of price*. Macmillan, New York, 1987, 371 p.

VARIAN, Hal R., 'Chapter 10: Price discrimination', in: R. Schmalensee and R. Willing (ed.), *Handbook of Industrial Organization.* Elsevier, Amsterdam, 1989, pp. 597-654.

VARIAN, Hal R., 'Economic Aspects of Personal Privacy', in: W. H. Lehr and L. M. Pupillo (ed.), *Internet Policy and Economics.* 2009, pp. 101-111.

YIN, Robert K., *Case Study Research - Design and Methods* (5th edition). SAGE Publications, Thousand Oaks, 2014, 282 p.

Journal Articles

AALBERTS, Robert J., NILL, Alexander & POON, Percy S., 'Online Behavioral Targeting: What Does the Law Say?', in: *Journal of Current Issues & Research in Advertising*, Vol.37, No.2, 2016, pp. 95-112.

ACAR, Gunes, et al., 'FPDetective: Dusting the web for fingerprinters', in: *Conference: Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, 2013, pp. 1129-1140.

ACQUISTI, Alessandro, BRANDIMARTE, Laura & LOEWENSTEIN, George, 'Privacy and human behavior in the age of information', in: *Science*, Vol.347, No.6221, 2015, pp. 509-514.

ACQUISTI, Alessandro, TAYLOR, Curtis R. & WAGMAN, Liad, 'The Economics of Privacy', in: *Journal of Economic Literature*, Vol.52, No.2, 2016, pp. 1-64.

ACQUISTI, Alessandro & VARIAN, Hal R., 'Conditioning Prices on Purchase History.', in: *Marketing Science*, Vol.24, No.3, 2005, pp. 367-381.

ASCARZA, E. V. A., IYENGAR, Raghuram & SCHLEICHER, Martin, 'The Perils of Proactive Churn Prevention Using Plan Recommendations: Evidence from a Field Experiment', in: *Journal of Marketing Research (JMR)*, Vol.53, No.1, 2016, pp. 46-60.

BAARSLAG, Tim, et al., 'When Will Negotiation Agents Be Able to Represent Us? The Challenges and Opportunities for Autonomous Negotiators', in: *Twenty-Sixth International Joint Conference on Artificial Intelligen*, Melbourne, 2017, pp. 4684-4690.

BAYE, Michael R., et al., 'A Dashboard for Online Pricing', in: *California Management Review*, Vol.50, No.1, 2007, pp. 202-216.

CALO, Ryan, 'Digital Market Manipulation', in: *George Washington Law Review*, Vol.82, No.4, 2014, pp. 995-1051.

CAMPBELL, James, GOLDFARB, Avi & TUCKER, Catherine E., 'Privacy Regulation and Market Structure', in: *Journal of Economics & Management Strategy*, Vol.24, No.1, 2015, pp. 47-73.

CASTELVECCHI, Davide, 'Can we open the black box of AI?', in: *Nature News*, Vol.538, No.7623, 2016, pp. 20.

CHOE, Chongwoo, KING, Stephen & MATSUSHIMA, Noriaki, 'Pricing with Cookies: Behavior-Based Price Discrimination and Spatial Competition', in: *Management Science*, pp. 1-34.

COHEN, Shlomo, 'Nudging and Informed Consent', in: *The American Journal of Bioethics*, Vol.13, No.6, 2013, pp. 3-11.

CRAWFORD, Kate & SCHULTZ, Jason, 'Big Data and Due Process: Toward a Framework to Redress Predictive Privacy', in: *Boston College Law Review*, Vol.55, No.1, 2014, pp. 93-128.

DATTA, Anupam, et al., 'Proxy Discrimination in Data-Driven Systems', in: *Theory and Experiments with Machine Learnt Programs*, 2017, pp. 1-14.

DE HERT, Paul, et al., 'The right to data portability in the GDPR: Towards user-centric interoperability of digital services', in: *Computer Law & Security Review*, Vol.34, No.2, 2018, pp. 193-203.

DE MONTJOYE, Yves-Alexandre, et al., 'Unique in the Crowd: The privacy bounds of human mobility', in: *Scientific Reports*, Vol.3, 2013, pp. 1-4.

DE NIJS, Romain, 'Behavior-based price discrimination and customer information sharing', in: *International Journal of Industrial Organization*, Vol.50, 2017, pp. 319-334.
DONGHYUN, Park, 'Price Discrimination, Economies of Scale, and Profits', in: *Journal of Economic Education*, Vol.31, No.1, 2000, pp. 66-75.
EVERSON, Eric, 'Privacy by design: Taking CTRL of Big Data', in: *Cleveland State Law Review*, Vol.65, No.1, 2017, pp. 27-43.
GERADIN, Damien & PETIT, Nicolas, 'Price discrimination under EC competition law: Another antitrust doctrine in search of limiting principles?', in: *Journal of Competition Law & Economics*, Vol.2, No.3, 2006, pp. 479-531.
GOLDFARB, Avi & TUCKER, Catherine E., 'Privacy Regulation and Online Advertising', in: *Management Science*, Vol.57, No.1, 2011, pp. 57-71.
GOODMAN, Bryce W., 'A Step Towards Accountable Algorithms?: Algorithmic Discrimination and the European Union General Data Protection', in: *29th Conference on Neural Information Processing Systems*, Barcelona, 2016, pp. 9.
GRAEF, Inge, VERSCHAKELEN, Jeroen & VALCKE, Peggy, 'Putting the Right to Data Portability into a Competition Law Perspective', in: *The Journal of the Higher School of Economics Annual Review*, 2013, pp. 53-63.
HANNAK, Aniko, et al., 'Measuring Price Discrimination and Steering on E-commerce Web Sites', in: *Proceedings of the 2014 Conference on Internet Measurement Conference*, Vancouver, BC, Canada, 2014, pp. 305-318.
HEURIX, Johannes, et al., 'A taxonomy for privacy enhancing technologies', in: *Computers & Security*, Vol.53, 2015, pp. 1-17.
IKEDA, Takeshi & NARIU, Tatsuhiko, 'Third-Degree Price Discrimination in the Presence of Asymmetric Consumption Externalities', in: *Journal of Industry, Competition and Trade*, Vol.9, No.3, 2009, pp. 251-261.
KAPTEIN, Maurits & PARVINEN, Petri, 'Advancing E-Commerce Personalization: Process Framework and Case Study', in: *International Journal of Electronic Commerce*, Vol.19, No.3, 2015, pp. 7-33.
KEATS CITRON, Danielle & PASQUALE, Frank, 'The scored society: Due process for automated predictions', in: *Washington Law Review*, Vol.89, No.1, 2014, pp. 1-33.
KOOPS, Bert-Jaap, 'Forgetting Footprints, Shunning Shadows: A Critical Analysis of the 'Right to Be Forgotten' in Big Data Practice', in: *Tilburg Law School Research Paper No. 08/2012*, Vol.8, No.3, 2012, pp. 1-27.
L. OLIVER, Richard & SHOR, Mikhael, 'Digital Redemption of Coupons: Satisfying and Dissatisfying Effects of Promotion Codes', in: *Journal of Product & Brand Management*, Vol.12, No.2, 2003, pp. 121-134.
LAYSON, Stephen K., 'Market-Opening under Third Degree Price Discrimination', in: *Journal of Industrial Economics*, Vol.42, No.3, 1994, pp. 335.
NORMAN, George, et al., 'Competition and consumer data: The good, the bad, and the ugly', in: *Research in Economics*, Vol.70, No.4, 2016, pp. 752-765.
OKADA, Tomohisa & ADACHI, Takanori, 'Third-Degree Price Discrimination, Consumption Externalities, and Market Opening', in: *Journal of Industry, Competition and Trade*, Vol.13, No.2, 2013, pp. 209-219.
OOSTVEEN, Manon, 'Identifiability and the applicability of data protection to big data', in: *International Data Privacy Law*, Vol.6, No.4, 2016, pp. 299-309.

RAYNA, Thierry, DARLINGTON, John & STRIUKOVA, Ludmila, 'Pricing music using personal data: mutually advantageous first-degree price discrimination', in: *Electronic Markets*, Vol.25, No.2, 2015, pp. 139-154.
RAZA, Syed Asif, 'An integrated approach to price differentiation and inventory decisions with demand leakage', in: *International Journal of Production Economics*, Vol.164, 2015, pp. 105-117.
RYZ, Lawrence & GREST, Lauren, 'A new era in data protection', in: *Computer Fraud & Security*, Vol.2016, No.3, 2016, pp. 18-20.
SELBST, Andrew D. & POWLES, Julia, 'Meaningful information and the right to explanation', in: *International Data Privacy Law*, Vol.7, No.4, 2017, pp. 233-242.
SENIČAR, Vanja, JERMAN-BLAŽIČ, Borka & KLOBUČAR, Tomaž, 'Privacy-Enhancing Technologies—approaches and development', in: *Computer Standards & Interfaces*, Vol.25, No.2, 2003, pp. 147-158.
SHOR, Mikhael & OLIVER, Richard L., 'Price discrimination through online couponing: Impact on likelihood of purchase and profitability', in: *Journal of Economic Psychology*, Vol.27, No.3, 2006, pp. 423-440.
SPIEKERMANN, Sarah, 'Individual Price Discriminaton in E-Commerce – An impossibility?', in: *Humboldt University Institute of Information Systems Research Paper* 2018, pp. 1-6.
STEPPE, Richard, 'Online price discrimination and personal data: A General Data Protection Regulation perspective', in: *Computer Law & Security Review*, Vol.33, No.6, 2017, pp. 768-785.
SUH, Eunju & ALHAERY, Matt, 'Customer Retention: Reducing Online Casino Player Churn Through the Application of Predictive Modeling', in: *UNLV Gaming Research & Review Journal*, Vol.20, No.2, 2016, pp. 63-83.
TAYLOR, C. R., 'Consumer privacy and the market for customer information', in: *The RAND Journal of Economics*, Vol.35, No.4, 2004, pp. 631-650.
VILLARONGA, Eduard Fosch, KIESEBERG, Peter & LI, Tiffany, 'Humans forget, machines remember: Artificial intelligence and the Right to Be Forgotten', in: *Computer Law & Security Review*, Vol.34, No.2, 2018, pp. 304-313.
VILLAS-BOAS, J., 'Price Cycles in Markets with Customer Recognition', in: *The Rand Journal of Economics*, Vol.35, No.3, 2004, pp. 486-501.
WACHTER, Sandra, MITTELSTADT, Brent & FLORIDI, Luciano, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation', in: *International Data Privacy Law*, 2017, pp. 1-47.
WOHLFARTH, Michael, 'Data Portability on the Internet: An Economic Analysis', in: *28th European Regional Conference of the International Telecommunications Society (ITS): "Competition and Regulation in the Information Age"*, Passau, 2017, pp. 1-24.
YEUNG, Karen, '‘Hypernudge’: Big Data as a mode of regulation by design', in: *Information, Communication & Society*, Vol.20, No.1, 2017, pp. 118-136.
ZHAO, Xia & XUE, Ling, 'Competitive Target Advertising and Consumer Data Sharing', in: *Journal of Management Information Systems*, Vol.29, No.3, 2012, pp. 189-222.
ZUIDERVEEN BORGESIUS, Frederik J., 'Singling out people without knowing their names – Behavioural targeting, pseudonymous data, and the new Data Protection Regulation', in: *Computer Law & Security Review*, Vol.32, No.2, 2016, pp. 256-271.

ZUIDERVEEN BORGESIUS, Frederik & POORT, Joost, 'Online Price Discrimination and EU Data Privacy Law', in: *Journal of Consumer Policy*, Vol.40, No.3, 2017, pp. 347-366.

Reports

Article 29 Working Party, *A29WP Opinion 2/2010 on online behavioural advertising*, Brussels, 2010, 24 p.

Article 29 Data Protection Working Party, *A29WP Opinion 4/2007 on the concept of personal data* Brussels, 2007, 26 p.

Information Commissioner's Office, *Big data, Artificial Intelligence, Machine Learning and Data Protection*, Wilmslow, 2017, 114 p.

Microsoft France, *GDPR - Get Organized and Implement the Right Processes for Compliance with the GDPR*, Issy-Les-Moulineaux, 2017, 69 p.

IAPP, *Geting to GDPR Compliance: Risk Evaluation and Strategies for Mitigation*, Portsmouth, 2018, 10 p.

Article 29 Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, Brussels, 2017, 34 p.

Article 29 Working Party, *Guidelines on consent under Regulation 2016/679*, 31 p.

Article 29 Working Party, *Guidelines on the right to "data portability"*, Brussels, 2017, 20 p.

Article 29 Working Party, *Guidelines on Transparency under Regulation 2016/679*, Brussels, 2018, 40 p.

Executive Office of the President; National Science and Technology Council; Committee on Technology, *Preparing for the Future of AI*, Washington D.C., 2016, 48 p.

D' ACQUISITO, Giuseppe, et al., ENISA, *Privacy by Design in Big Data. An Overview of Privacy Enhancing Technologies in the Era of Big Data Analytics.*, Heraklion, 2015, 80 p.

Newspaper Articles

DICKSON, Ben, 'What is Narrow, General and Super Artificial Intelligence?', *TechTalks*, 12th May 2017, Available at: https://bdtechtalks.com/2017/05/12/what-is-narrow-general-and-super-artificial-intelligence (consulted on 16.4.2018)

INGOLD, David & SOPER, Spencer, 'Amazon Doesn't Consider the Race of Its Customers. Should It?', *Bloomberg*, 21st April 2016, Available at: https://www.bloomberg.com/graphics/2016-amazon-same-day (consulted on 16.4.2018)

LANDES, Harlan, 'Individualized Coupons Aid Price Discrimination', *Forbes*, 21 August 2012, Available at: https://www.forbes.com/sites/moneybuilder/2012/08/21/individualized-coupons-aid-price-discrimination/#26c20f8a45e7 (consulted on 27.4.2018)

ROSENCRANCE, Linda, 'Customer outrage prompts Amazon to change price-testing policy', *Computerworld*, 13 September 2000, Available at: https://www.computerworld.com/article/2597088/retail-it/customer-outrage-prompts-amazon-to-change-price-testing-policy.html (consulted on 7.4.2018)

SCHRAGE, Michael, 'Big Data's Dangerous New Era of Discrimination', *Harvard Business Review*, 29 January 2014, Available at: https://hbr.org/2014/01/big-datas-dangerous-new-era-of-discrimination (consulted on 25.4.2018)

SCOTT, Mark & CERULUS, Laurens, 'Europe's new data protection rules export privacy standards worldwide', *Politico Europe*, 31 January 2018, Available at: https://www.politico.eu/article/europe-data-protection-privacy-standards-gdpr-general-protection-data-regulation (consulted on 28.3.2018)

Websites and Online Reports

BrightPrice Suite, Available at: http://www.sposea.com/bright-price-suite.html#pdm (consulted on 27.2.2018).

Darwin Pricing, *Case Study: Worldwide Cyclery*, Available at: https://www.darwinpricing.com/sales/brochures/case-studies/worldwide-cyclery/en/Case_Study_Worldwide_Cyclery.pdf (consulted on 8.5.2018).

Dynamic Pricing Software for Geo-Targeted eCommerce, Available at: https://www.darwinpricing.com/de/geo-targeted-ecommerce (consulted on 27.4.2018).

European Commission, *EU Data Protection Reform: better rules for European businesses*, Available at: https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-business_en.pdf (consulted on

DLA Piper Global Law Firm, *EU General Data Protection Regulation - Key changes* Available at: https://www.dlapiper.com/en/uk/focus/eu-data-protection-regulation/key-changes/#higher%20bar (consulted on 26.5.2018).

Economics Online, *Price discrimination as a profit maximising strategy*, Available at: http://economicsonline.co.uk/Business_economics/Price_discrimination.html (consulted on 2018/02/18/).

Darwin Geo-Pricing, *Price for Profit with the World's Leading Dynamic Pricing Solution For Geo-Targeted Price Optimization*, Available at: https://www.darwinpricing.com/de/ (consulted on 7.5.2018).

Techopedia, *What is a Flash Cookie?*, Available at: https://www.techopedia.com/definition/23464/flash-cookie (consulted on 5.4.2018).

Gartner IT Glossary, *What Is Big Data?*, Available at: https://www.gartner.com/it-glossary/big-data (consulted on 4.3.2018).

Techopedia, *What is Web Scraping?*, Available at: https://www.techopedia.com/definition/5212/web-scraping (consulted on 5.1.2018).

ALDERIGHI, Marco, GAGGERO, Alberto A. & PIGA, Claudio A., *The hidden sides of 'dynamic pricing' for airline tickets.* LSE Business Review, 2017, Available at: http://blogs.lse.ac.uk/businessreview/2017/05/10/the-hidden-sides-of-dynamic-pricing-for-airline-tickets (consulted on 6.4.2017)

BOZHANOV, Bozhidar, *Tracking Cookies and GDPR.* 2018, Available at: https://dzone.com/articles/tracking-cookies-and-gdpr (consulted on 29.4.2018)

CHRISTENSSEN, Per, *IP Address Definition.* Tech Terms, 2018, Available at: https://techterms.com/definition/ip_address (consulted on 24.03.2018)

European Commission, *Data Protection - better rules for small business*, Available at: http://ec.europa.eu/justice/smedataprotect/index_en.htm (consulted on 6.2.2018).

Ecommerce Europe, *The General Data Protection Regulation is now a reality!*, Available at: https://www.ecommerce-europe.eu/news-item/the-general-data-protection-regulation-is-now-a-reality/ (consulted on 6.2.2018)

JACOBS, Sven & RITZER, Christoph, *Data privacy: AI and the GDPR.* Norton Rose Fulbright, 2017, Available at: https://aitech.law/blog/data-privacy-ai-and-the-gdpr (consulted on 6.5.2018)

KOLLMANN, Tobias, *Definition: Cookie.* Gabler Wirtschaftslexikon, 2018, Available at: https://wirtschaftslexikon.gabler.de/definition/cookie-27577 (consulted on 24.03.2018)

KOTULA, Marcin, *IP addresses as personal data - the CJEU's judgment in C-582/14 Breyer*. EU-Law Analysis, 2017, Available at: https://eulawanalysis.blogspot.com/2017/01/ip-addresses-as-personal-data-cjeus.html (consulted on 3.4.2018)

MERLER, Silvia, *Big data and first-degree price discrimination.* Bruegel, 2017, Available at: http://bruegel.org/2017/02/big-data-and-first-degree-price-discrimination (consulted on

O'REILLY, Tim, *What Is Web 2.0.* 2018, Available at: http://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html?page=1 (consulted on 15.2.2018)

PERUGINI, Maria Roberta, *Personal Data made public by the Data Subject and use of Information on Social Networks.* Europrivacy, 2016, Available at: http://europrivacy.info/2016/10/31/personal-data-made-public-by-the-data-subject-and-use-of-information-published-on-social-networks-initial-observations-of-the-gdpr-art-9-para-2-letter-e-seco (consulted on 1.5.2018)