AFFINITY-BASED ALGORITHMIC PRICING

A DILEMMA FOR EU DATA PROTECTION LAW

CREATe Working Paper 2022/9

ZIHAO LI

CREATe

Affinity-based Algorithmic Pricing: A Dilemma for EU Data Protection Law

Zihao Li*

Abstract

The emergence of big data and machine learning has allowed sellers and online platforms to tailor pricing for customers in real-time, but as many legal scholars have pointed out, personalised pricing poses a threat to the fundamental values of privacy and non-discrimination, raising legal and ethical concerns. However, most of those studies neglect affinity-based algorithmic pricing, which may bypass the General Data Protection Regulation (GDPR). This paper evaluates current data protection law in Europe against online algorithmic pricing. The first contribution of the paper is to introduce and clarify the term "online algorithmic pricing" in the context of data protection legal studies, as well as a new taxonomy of online algorithmic pricing by processing the data types. In doing so, the paper finds that the legal nature of affinity data is hard to classify as personal data. Therefore, affinity-based algorithmic pricing is highly likely to circumvent the GDPR. The second contribution of the paper is that it points out that even though some types of online algorithmic pricing can be covered by the GDPR, the data rights provided by the GDPR struggle to provide substantial help. **The key finding of this paper is that the GDPR fails to apply to affinity-based algorithmic pricing, but the latter still can lead to privacy invasion.** Therefore, four potential resolutions are raised, relating to group privacy, the remit of data protection law, the ex-ante measures in data protection, and a more comprehensive regulatory approach.

Keywords

Data protection law, Online algorithmic pricing, Personalised pricing, GDPR, Affinity-based pricing, Artificial Intelligence Act

* Zihao Li is a PhD researcher and research assistant at CREATe Centre, School of Law, University of Glasgow and a recipient of a Modern Law Review (MLR) Scholarship. The author would like to thank Prof. Martin Kretschmer, Dr. Luis Porangaba and Prof. Thomas Margoni for their valuable comments, suggestions and supervision. The author is also grateful to the editors and anonymous reviewers of the Journal of Computer Law and Security Review (CLSR) for their comments and suggestions. The link of submission in CLSR: https://doi.org/10.1016/j.clsr.2022.105705

1. Introduction

The development of big data and machine learning techniques has enabled online platforms to generate users' digital profiles or infer their status by collecting and processing unprecedented volumes of data, which can strengthen sellers' ability to provide tailored and personalised prices to customers.[1] For example, as early as 2001 Amazon was reportedly using cookies data to analyse customer behaviours, then selling products to different users for different prices.[2] In 2012, consumers again discovered that the prices charged for items on Amazon.com are highly variable, as reported by an Oregon newspaper.[3] A consumer placed a set of mahjong tiles offered at $54.99 into her online shopping basket, but a few minutes later noticed that the item had jumped to $79.99 in her basket, and that when she cleared the cart and tried again, the item was priced at $59.99.[4] Meanwhile, Staples Inc.'s website is reported to present various rates to consumers based on their estimated location. Staples.com frequently displayed lower pricing if competing shops were physically situated within around 20 miles of the customer's estimated location.[5] All these examples build users' digital footprints and employ machine learning algorithms to anticipate the price that end users will be willing to pay for products or services.

Owing to the increasing problems of privacy invasion, loss of control of informational self-determination, and the inequality and unfairness caused by the uncertainty of legal regulation in this grey area, many professionals have called for legal interventions to counter the commonly applied practice of algorithmic pricing, which is ubiquitous in the business world, because it can lead to severe infringement of users' fundamental rights.[6] In the European Union (EU), for

---

[1] UK Competition and Markets Authority, 'Pricing Algorithms: Economic Working Paper on the Use of Algorithms to Facilitate Collusion and Personalised Pricing' [2018] UK Competition and Markets Authority Working Paper. <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/746353/Algorithms_econ_report.pdf>; Adam Ozimek, 'Will Big Data Bring More Price Discrimination?' (*Forbes*, 2013): <https://www.forbes.com/sites/modeledbehavior/2013/09/01/will-big-data-bring-more-price-discrimination/?sh=53521dbe2cb1> accessed 3 November 2020.

[2] Mark Ward, 'BBC News | BUSINESS | Amazon's Old Customers "Pay More"' (*BBC News*, 2000): <http://news.bbc.co.uk/1/hi/business/914691.stm> accessed 9 March 2021.

[3] Laura Gunderson, 'Amazon's "dynamic" Prices Get Some Static' (*The Oregonian*, 2012): <https://www.oregonlive.com/complaintdesk/2012/05/amazons_dynamic_prices_get_som.html> accessed 3 January 2022.

[4] Ibid.

[5] Tim Worstall, 'Why Does Online Pricing Discriminate?' (*Forbes*, 2012): <https://www.forbes.com/sites/timworstall/2012/12/25/why-does-online-pricing-discriminate/> accessed 3 January 2022; See also Christopher Townley, Eric Morrison and Karen Yeung, 'Big Data and Personalized Price Discrimination in EU Competition Law' (2017) 36 Yearbook of European Law 683, 1–2.

[6] UK Competition and Markets Authority (n 1). Executive Office of the President of the United States, 'Big Data and Differential Pricing' [2015] Whitehouse.Gov 1: <https://www.whitehouse.gov/sites/default/files/docs/Big_Data_Report_Nonembargo_v2.pdf>. Peter Seele and others, 'Mapping the Ethicality of Algorithmic Pricing: A Review of Dynamic and Personalized

example, the data protection law can hopefully regulate online personalised pricing by indirectly controlling personal data usage and preventing the data subject from being subject to algorithms.[7] However, among the discussions on applying the General Data Protection Regulation (GDPR) to online algorithmic pricing, economic terms such as "price discrimination" and "personalised pricing" may contain potential bias when used to describe online algorithmic pricing in the legal area, since not all personalised pricing is detrimental, and indeed not all algorithmic pricing is personalised.[8] Besides, the usage of such terms neglects affinity data-based online algorithmic pricing, which may erode the foundation of the GDPR,[9] because the risks raised by the uncertainty of legal nature of affinity data and inference are mostly not considered.[10]

This paper firstly discusses the limitations of the terms "personalised pricing" and "price discrimination" in the legal research before proposing a new concept to improve the law. Based on the new concept, namely online algorithmic pricing, a detailed taxonomy is offered by following the method used in data protection law, which provides the basis for the subsequent legal analysis. Through this taxonomy, a new form of online algorithmic pricing, namely affinity-based pricing algorithm, is disclosed. An example of this way of pricing is Uber, which is known to charge users with low-battery phones more, as they may be more desperate.[11] This new application may completely bypass the GDPR because battery information cannot identify

---

Pricing' (2021). 170 Journal of Business Ethics 697 <https://doi.org/10.1007/s10551-019-04371-w>. Joshua A Gerlick and Stephan M Liozu, 'Ethical and Legal Considerations of Artificial Intelligence and Algorithmic Decision-Making in Personalized Pricing' (2020) 19 Journal of Revenue and Pricing Management 85 <https://doi.org/10.1057/s41272-019-00225-2>.

[7] Frederik Zuiderveen Borgesius and Joost Poort, 'Online Price Discrimination and EU Data Privacy Law' (2017) 40 Journal of Consumer Policy 347, 356. The reason why data protection law should apply to this issue is discussed in detail in Section 2.

[8] Akiva A Miller, 'What Do We Worry About When We Worry About Price Discrimination? The Law and Ethics of Using Personal Information for Pricing' (2014) 19 Journal of Technology Law and Policy 41; Richard Steppe, 'Online Price Discrimination and Personal Data: A General Data Protection Regulation Perspective' (2017) 33 Computer Law and Security Review 768: <https://doi.org/10.1016/j.clsr.2017.05.008>; Zuiderveen Borgesius and Poort (n 7). Benjamin Wong, 'Online Personalised Pricing as Prohibited Automated Decision-Making under Article 22 GDPR: A Sceptical View' (2021) 30 Information & Communications Technology Law 193 <https://doi.org/10.1080/13600834.2020.1860460>.

[9] Jessica Lindsay, 'Does Uber Charge More If Your Battery Is Lower?' (*Metro News*, 2019): <https://metro.co.uk/2019/09/27/uber-charge-battery-lower-10778303/> accessed 3 November 2020; Amit Chowdhry, 'Uber: Users Are More Likely To Pay Surge Pricing If Their Phone Battery Is Low' (*Forbes*, 2016) <https://www.forbes.com/sites/amitchowdhry/2016/05/25/uber-low-battery/?sh=6a42480574b3> accessed 3 November 2020; Nicole Martin, 'Uber Charges More If They Think You're Willing To Pay More' (*Forbes*, 2019) <https://www.forbes.com/sites/nicolemartin1/2019/03/30/uber-charges-more-if-they-think-youre-willing-to-pay-more/?sh=7f9256c57365> accessed 3 November 2020.

[10] Monique Mann and Tobias Matzner, 'Challenging Algorithmic Profiling: The Limits of Data Protection and Anti-Discrimination in Responding to Emergent Discrimination' (2019) 6 Big Data and Society. Seele and others (n 6).

[11] Chowdhry (n 9); Lindsay (n 9); Martin (n 9).

a specific user. Therefore, it is argued that this new form of algorithmic pricing may pose a new threat that undermines the protection offered by the GDPR.

Although it is not advisable to prohibit online algorithmic pricing from the perspectives of economics and market liberalism,[12] further legal intervention is still necessary if privacy intrusion and unfair treatment occurs.[13] The proposed taxonomy identifies the most two privacy-intruding forms of algorithmic pricing. The paper then examines the extent to which the GDPR can be applied to the two types of online algorithmic pricing, pointing out the loophole of the dichotomy of personal data in the context of online algorithmic pricing. Furthermore, the paper examines the protection that the GDPR can provide to individuals in the context of online algorithmic pricing. The analysis includes the right to know about (Articles 13–15), right to rectify (Article 16), right to delete (Article 17), right to object (Article 21), and the right not to be subject to automatic decision-making (Article 22). This overview explains why the current digital rights under the GDPR cannot work as expected in the context of online algorithmic pricing.

Finally, as the current regime in the EU is insufficient to handle online algorithmic pricing, a new dynamic classification approach through so-called "group privacy" is required to improve data protection law, because group privacy can protect data subjects who are not singled out as individuals but as members of a group. Meanwhile, it is also suggested that the remit of the law should be broadly interpreted by the CJEU and agree with Article 29 Working Party (hereafter: Art. 29 WP). Furthermore, as it is impossible to prohibit online algorithmic pricing, it is important to recognise transparency and the preceding evaluation in setting prices as the key to tackling the issue. Thus, ex-ante measures in data protection law should be used to increase the transparency and mitigate the potential risks to ensure that online algorithmic pricing is pro-competition and pro-consumers. Both the ex-ante and ex-post mechanisms should grant data subjects more control over their own data, thereby returning the autonomy of private decision-making to individuals. However, data protection law is not enough to regulate this issue alone; it is necessary to form a comprehensive regulatory approach by combining consumer protection law, competition law, data protection law, and anti-discrimination law.

[12] UK Office of Fair Trading, Patrick Coen and Natalie Timan, 'The Economics of Online Personalised Pricing' [2013] Office of Fair Trading Working Paper 97: <https://webarchive.nationalarchives.gov.uk/20140402154756/http:/oft.gov.uk/shared_oft/research/oft1488.pdf>.

[13] The reasons for the need for further legal intervention are discussed in Section 2.

2. Why Data Protection Law Should Apply to Online Algorithmic Pricing

Several legal domains may offer responses to growing public concerns about online algorithmic pricing. Competition law and customer protection law are obvious options, given that online algorithmic pricing could cause algorithmic collusion[14] via market monopoly, as well as clearly infringing the interests of customers[15]. Meanwhile, other areas of law could also cover this issue, for example e-commerce law[16] and anti-discrimination law[17]. However, this paper intends to critically examine these practices from the perspective of data protection law, for the following three reasons.

Firstly, online algorithmic pricing relies heavily on the direct or indirect collection and algorithmic processing of personal data and data that could reveal certain aspects of a user's status, automatically triggering data protection law and falling into its scope. Also, following the interpretation of personal data in Art. 29 WP and the CJEU, "everything could be personal data".[18] Therefore, data protection law should be the obvious candidate.

Secondly, the purpose and aim of modern data protection law are to protect individual privacy and identity,[19] equality, reputation, and informational self-determination.[20] However, online algorithmic pricing and related machine learning often provide new opportunities for privacy-invasion, discrimination and loss of informational autonomy. Privacy is the first thing to be threatened by algorithmic pricing, because most algorithmic pricing relies on behavioural data (browsing duration, click rate, etc.) and personal data (e.g. browsing history, shopping history, address, etc.) to generate prices. Some algorithmic pricing can even infer a user's status from affinity data, revealing sensitive information and predictions about their private life, behaviours,

[14] Antonio Capobianco and Pedro Gonzaga, 'Competition Challenges of Big Data: Algorithmic Collusion, Personalised Pricing and Privacy', *Legal Challenges of Big Data* (Edward Elgar Publishing 2020): <https://www.elgaronline.com/view/edcoll/9781788976213/9781788976213.00008.xml>.

[15] Natali Helberger, Frederik Zuiderveen Borgesius and Agustin Reyna, 'The Perfect Match? A Closer Look at the Relationship between EU Consumer Law and Data Protection Law' (2017) 54 Common Market Law Review 1427.

[16] Jiangqiu GE and Li CHEN, 'The Obligation to Provide "Non-Personalised" Search Results under the Chinese E-Commerce Law' (2021) 41 Computer Law & Security Review 1: <https://linkinghub.elsevier.com/retrieve/pii/S0267364921000418>.

[17] F Zuiderveen Borgesius, 'Price Discrimination, Algorithmic Decision-Making, and European Non-Discrimination Law' (2020) 31 European Business Law Review 401: <https://www.scopus.com/inward/record.uri?partnerID=HzOxMe3b&scp=85100671800&origin=inward>.

[18] Nadezhda Purtova, 'The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law' (2018) 10 Law, Innovation and Technology 40, 41–43: <https://www.tandfonline.com/doi/full/10.1080/17579961.2018.1452176>.

[19] Brent Mittelstadt, 'From Individual to Group Privacy in Big Data Analytics' (2017) 30 Philosophy and Technology 475–477.

[20] Lilian Edwards and Michael Veale, 'Slave to the Algorithm? Why a Right to Explanationn Is Probably Not the Remedy You Are Looking For' (2017) 16 Duke Law & Technology Review 18, 73.

health conditions, and private preferences.[21] The misuse of such technology jeopardises users' privacy and erodes their right to informational self-determination. Furthermore, online algorithmic pricing may create more opportunities for discrimination and biased decisions. Most pricing algorithms have a high tolerance of mistakes, and the prices generated by algorithms have no guarantee of accuracy or certainty. In some cases, the criterion for price-making is very simple,[22] meaning they are likely to cause discrimination and bias. Meanwhile, unlike decisions made by humans, Big Data analytics are deployed ubiquitously and can collect data from almost anywhere for long-term assessment. Such predictions may persist over time and solidify as someone's identity and reputation in the future. Also, the profile established by algorithms can be used to nudge and manipulate individuals without their knowledge,[23] infringing their informational self-determination. The misuse of such technology apparently contravenes the principles of data protection law, i.e., fairness, lawfulness, and transparency. Thus, data protection law should prevent the misuse of such technology and provide remedies to individuals.

Thirdly, compared with other legislation (e.g. competition law or consumer protection law), data protection law has its own advantages in providing remedies to individuals. Data protection not only focuses on ex-post legal remedy (i.e., after an infringement has occurred, the data subject can assert their empowered data rights), but also provides relevant ex-ante measures by taking a risk-based approach to prevent the misuse of personal data. For example, Data Protection Impact Assessment (DPIAs) and Data Protection by Design and Default (DPbD) can detect the potential risks of algorithms before they cause violations. Such ex-ante mechanisms have the potential to resolve issues before the deployment of technology.[24] Moreover, data protection law could provide a unique lens for interrogating the chilling effects of online algorithmic pricing. In consumer protection law, the individual must become the customer so that they can seek legal redress against online algorithmic pricing. However, before a user becomes a customer, if they think they are being monitored or tracked, most people will have to carefully control their own online activity as a means to restrict their online profiling.[25] This could have a negative effect on

[21] Yuxiao Dong and others, 'Inferring User Demographics and Social Strategies in Mobile Social Networks', *Proceedings of the 20th ACM SIGKDD international conference on Knowledge discovery and data mining* (ACM 2014) 15–16: <https://dl.acm.org/doi/10.1145/2623330.2623703>.
[22] For example, some platforms may use a customer's phone brand as a criterion to charge. This idea is discussed further below.
[23] Andreas Kapsner and Barbara Sandfuchs, 'Nudging as a Threat to Privacy' (2015) 6 Review of Philosophy and Psychology 455: <http://link.springer.com/10.1007/s13164-015-0261-4>.
[24] Yordanka Ivanova, 'The Data Protection Impact Assessment as a Tool to Enforce Non-Discriminatory AI', *Privacy Technologies and Policy* (2020): <http://link.springer.com/10.1007/978-3-030-55196-4_1>.
[25] Jiahong Chen, *Regulating Online Behavioural Advertising Through Data Protection Law* (Edward Elgar Publishing 2021) 84–85 <https://www.elgaronline.com/view/9781839108297.xml>.

user activity and expression which may prove detrimental to online society.[26] Data protection law does not have such a threshold. Even if the data subject does not purchase any product, data protection regulations still apply if their personal data is collected or processed.

3. The Concept of Online Algorithmic Pricing and the Legal Research on Data Protection Law

Various different terms have been used to address online algorithmic pricing, such as personalised pricing, price discrimination, and dynamic pricing.[27] One of the most popular definitions was provided by the Organisation for Economic Co-operation and Development (OECD), which defines online personalised pricing as the "practice of price discriminating final consumers based on their personal characteristics and conduct, resulting in prices being set as an increasing function of consumers' willingness to pay."[28] Table 1 summarises the four mainstream definitions of the terms, as used in data protection law studies. However, with the development of online algorithmic pricing, the scope of these definitions seems limited because they cannot cover algorithmic pricing that is not based on personal data, but on data that can indicate certain conditions of individuals.[29] For example, as was previously mentioned, Uber has been reported to charge users differently according to the battery information on their phones, based on the assumption that those with lower batteries are likely to be more desperate for immediate services.[30] Similar online personalised pricing also happens in China, where Meituan, one of the largest online travel apps, is known to charge its users according to their membership bands and phone brands;[31] iPhone users are charged more because they are believed to be wealthier and thus more willing to pay. Unfair as this may seem, neither the phone brand nor battery information seem to belong to the doctrinal category of personal data, let alone privacy, as such information cannot be used to identify or single out a specific individual.[32] These examples therefore reveal that the previous concepts are too limited to cover differential pricing

[26] Ibid.
[27] Joost Poort and Frederik Zuiderveen Borgesius, 'Personalised Pricing: The Demise of the Fixed Price?', *Data-Driven Personalisation in Markets, Politics and Law* (Cambridge University Press 2021): <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3792842>. Seele and others (n 6).
[28] Organisation for Economic Co-operation and Development (OECD), 'Personalised Pricing in the Digital Era', vol 33 (2018): <www.oecd.org/daf/competition/personalised-pricing-in-the-digital-era.htm%0Awww.oecd.org/daf/competition/market-concentration.htm.>.
[29] Seele and others (n 6).
[30] Lindsay (n 9). See also Martin (n 9).
[31]Sophie Yu and Brenda Goh, 'China Fines Group-Buying Platforms Owned by Meituan, Pinduoduo over Improper Pricing (*Reuters*, 2021): <https://www.reuters.com/article/us-china-group-buying-idUSKBN2AV0IL> accessed 9 March 2021.; See also Yajie Gao and Ai Deng Wei Han, 'Algorithmic Price Discrimination on Online Platforms and Antitrust Enforcement in China's Digital Economy' (2018) 2017 The Antitrust Source 1.
[32] Article 4(1), GDPR.

practices on an algorithm-created group level rather than a personal level. But as Steppe points out, the essence of online algorithmic pricing is that "the same provider sells identical products or service for different prices and such differences are not motivated by different cost structures (e.g. different costs of supply)."[33]

Table 1 Algorithmic pricing terms in recent studies on data protection law

Author (year)	Title	Terms & Definitions
Borgesius and Poort (2017, p.348)[34]	Online Price Discrimination and EU Data Privacy Law	Online price discrimination or personalised pricing: a practice that "differentiates the online price for identical products or services partly based on information a company has about a potential customer."
Steppe (2017, p.769)[35]	Online price discrimination and personal data: A General Data Protection Regulation perspective	Price discrimination: the practice of "[the] same provider sell[ing] identical products for different prices and such differences are not motivated by different cost structures (e.g. different costs of supply)."
Wong (2020, p.2)[36]	Online personalised pricing as prohibited automated decision-making under Article 22 GDPR: a sceptical view	Online personalised pricing: the practice of setting prices for customers "based on their personal characteristics and conduct, resulting in prices being set as an increasing function of customers' willingness to pay."
Poort and Borgesius (2021, p.2)[37]	Personalised Pricing: The Demise of the Fixed Price?	Online price discrimination: a situation in which "an online seller or platform is technically able to offer every consumer a different price for the same product, based on [the] information it has about the customers."

[33] Steppe (n 8).
[34] Zuiderveen Borgesius and Poort (n 7).
[35] Steppe (n 8).
[36] Wong (n 8).
[37] Poort and Borgesius (n 27).

Among all these terms, price discrimination is the common term used to describe such practice in both economic and legal areas. From a traditional economic perspective, price discrimination already exists in the offline world, which is often categorised into three types: first-degree price discrimination, second-degree price discrimination, and third-degree price discrimination.[38] First-degree price discrimination, also known as "perfect" price discrimination, is used to describe a situation where each consumer is charged the maximum of what one is willing to pay, which is "perfect" because it maximises the seller's profits.[39] However, this type of pricing was usually regarded as an impossibly idealistic scenario before the emergence of big data and data mining, where the online algorithmic pricing achieved by invading users' privacy seems similar to first-degree price discrimination. For example, a platform could collect someone's browsing history, shopping records, and postcode in order to automatically generate a user profile. Based on that profile, a platform can easily predict a user's willingness to pay, or switch and tailor prices accordingly. Second-degree price discrimination means the price is set depending on the quantity of purchases.[40] In other words, larger discounts are granted to bigger purchases. Lastly, in third-degree price discrimination, the price is set according to different consumer groups categorised by variables such as age, occupation, and gender.[41] This scenario is commonly seen when purchasing tickets at cinemas or tourist attractions, where students and the elderly can claim discounts.

Although price discrimination is already categorised, such a taxonomy is neither appropriate for legal analysis nor suitable in an online environment. Firstly, the word "discrimination" may lead to an ambiguous meaning in a legal context because it usually refers to the unjust or prejudicial treatment of different categories of people.[42] Not all types of algorithmic pricing are detrimental to the extent that they should be prohibited.[43] Advocates of algorithmic pricing claim that it can benefit customers on low incomes with discounts, which helps to increase social efficiency.[44] Similarly, the existing UK Office of Fair Trading (OFT) has failed to "conclude whether, in general, online personalised pricing is harmful or beneficial to consumers,"[45] because it is impossible to generalise the economic effects of online personalised pricing as the welfare outcomes are too highly dependent on different marketing variables.

[38] Townley, Morrison and Yeung (n 5).
[39] Ibid. See also Steppe (n 8).
[40] Ibid.
[41] Gerlick and Liozu (n 6).
[42] Borgesius (n 17) 9.
[43] UK Office of Fair Trading, Coen and Timan (n 12) 10–12; Wong (n 8) 11–14.
[44] Capobianco and Gonzaga (n 14). Miller (n 8).
[45] UK Office of Fair Trading, Coen and Timan (n 12) 11. See also UK Competition and Markets Authority (n 1).

Similarly, the fact that algorithmic pricing is not completely negative is also recognised by the EU's secondary legislation. According to Recital 45 of the Consumer Right Directive (CRD) Amending Directive, traders can personalise the price of their offers to specific individuals or groups via the profiling of customers' behaviours through automated decision-making, which makes it possible for traders to assess consumers' purchasing power. It is therefore safe to conclude that although algorithmic pricing can cause several problems, it is not sensible (or realistic) to abandon it altogether. In legal studies, the use of the word "discrimination" in data protection law, which is supposed to deal with fairness and transparency, may lead to bias, even though the term should be neutral. For example, Poort and Borgesius have illustrated that people normally see online price discrimination as unfair and unacceptable, and believe that it should be banned.[46] However, it is doubtful whether the concept of online price discrimination is properly understood, and if the word "discrimination" may have misled the public in the survey.[47] As Poort and Borgesius explained in their own survey, the term "discrimination" may be normatively loaded,[48] and its misuse may also ignore the positive side of "personalised pricing," including providing discounts for low-income groups and increasing social efficiency. For example, Poort and Borgesius's study shows that more customers are willing to accept price discrimination if a discount is involved,[49] which seems to contradict previous attitudes. To reiterate, the word "discrimination" in legal studies may contain potential bias that leads to ambiguity.

Meanwhile, the term "personalised pricing" also has notable drawbacks. Firstly, since not all algorithmic pricing uses personal data to provide personalised prices, the harmful side of algorithmic pricing is excluded, such as the harm caused by charging customers according to their battery level or phone brand. Secondly, instead of being personalised, some algorithmic pricing may be set by groups that are created by algorithm.[50] In other words, if a group of users shares similar behaviour, characteristics, and property, then the price algorithm will provide them with the same price, which means that the price is not personalised as such. Data collected by algorithm cannot be used to single out an individual, because many users share similar properties. Thirdly, the definition of personalised pricing should not broadly cover affinity-based algorithmic pricing, as this may lead legal scholars to neglect the affinity-based algorithmic pricing or to confuse affinity data-based algorithmic pricing with personal data-based

[46] Zuiderveen Borgesius and Poort (n 7) 355.
[47] Joost Poort and Frederik J Zuidervee Borgesius, 'Does Everyone Have a Price? Understanding People's Attitude towards Online and Offline Price Discrimination' (2019) 8 Internet Policy Review 6.
[48] Ibid.
[49] Ibid 7–9.
[50] Mann and Matzner (n 10); Mittelstadt (n 19).

algorithmic pricing. Such confusion needs to be clarified as the difference of these two types of online algorithmic pricing is the key for data protection legal analysis. Otherwise, legal scholars may continue to overlook the importance of the nature of affinity data and the inferences generated by it in the context of online algorithmic pricing. Therefore, since there is a trend towards convergence between personalised and dynamic pricing,[51] both personalised pricing and some types of dynamic pricing can raise ethical and legal issues.[52]

To sum up, it is suggested that an umbrella term "online algorithmic pricing"[53] should be used to replace "price discrimination," especially in legal studies. This can be defined as a price strategy based on data analysis which allows sellers to automatically generate different prices for individuals or groups in real-time. From an economic perspective, online algorithmic pricing can mean different types of price discrimination among individuals or groups. Although the analysis above discloses that it is not sensible to prohibit online algorithmic pricing per se, certain legal interventions are definitely needed, because such practices can be invasive to users' privacy and data protection rights by creating new windows for discrimination. For those types that are potentially harmful or which have an influence on individuals' privacy, legal intervention regarding information self-determination, autonomy, and equality should be promoted.

3.1. The Taxonomy of Online Algorithmic Pricing in Data Protection Law

Based on the above discussion, it is necessary to classify "personalised pricing" in relation to the legal aspect. With the method used in the data protection law regarding the dichotomy of personal data and non-personal data, this paper proposes three distinct categories of algorithmic pricing, namely personal data-based algorithms, non-personal data-based algorithms, and affinity-based algorithms.

[51] Dynamic pricing, also known as surge pricing or demand pricing, is a strategy whereby sellers set flexible prices for products or services based on the supply and demand relationship. The data used for dynamic pricing is normally non-personal in nature. For example, sellers can automatically set real-time prices through algorithms based on how many people are currently browsing the product and on the remaining level of product inventory.

[52] Seele and others (n 6).

[53] "Price differentiation" is another term used to replace the term "personalised pricing" and "price discrimination". However, price differentiation cannot distinguish whether the decision on price-making has been made by a human or an algorithm, which may lead to a completely different legal response. See the detailed discussion in section 6.4, which discusses the premises to apply the right to object and not be subject to automated decision-making.

Table 2 Taxonomy of online algorithmic pricing

Type of algorithmic pricing	The processed data	Exemplar uses
Personal data-based algorithmic pricing	Dynamic and Static IP address, various cookies, MAC address, IDFA & IDFV (for Apple products), Device ID (for Android products)	Amazon uses cookies to analyse consumers' browsing history to set prices.
Non-personal data-based algorithmic pricing	Weather, Demand and Require, Delivery Address (to satisfy the purpose limitation principle), time of day, website traffic, historical data, or competitor's prices	Some airlines charge their customers according to seasons or choices of seats.
Affinity-based algorithmic pricing (Group Privacy)	The nature of the data is unclear and may not be covered by data protection law. However, many aspects can be considered influential, such as membership and phone battery information.	Uber charges according to customers' phone batteries; Meituan sets prices based on customers' phone brands

These three different types of algorithmic pricing are illustrated in Table 2. Personal data-based algorithm pricing, or personalised pricing, is the type which online platforms or sellers generally deploy to create user profiles by collecting users' behavioural data. For example, as was mentioned above, Amazon uses cookies data to establish a user profile and then charges different prices to different users according to their profile and behaviours.[54] Nowadays, after more than two decades of online retail, it is still hard to prevent this from happening because of the opacity of the algorithms and data processing techniques of internet giants. Likewise, in the insurance industry, data from social media is processed to build user profiles for risk assessments, which will then determine the price of the insurance policy.[55]

[54] Ward (n 2).

[55] Brendan McGurk, *Data Profiling and Insurance Law* (Hart Publishing 2019): <https://www.bloomsburycollections.com/book/data-profiling-and-insurance-law>.

In non-personal data-based algorithmic pricing, the data that the price algorithms use to set prices is unrelated to customers' privacy.[56] For example, variables that determine pricing can include the weather, level of demand, the season, the time of the day, and historical price data.

This technique is most commonly found in transportation businesses' websites. Also, some airlines charge customers according to their choices of seats.[57] Similarly, Uber adopts a "surge pricing" system, charging more in bad weather or heavy traffic.[58]

Affinity-based algorithmic pricing is regarded as an emerging kind of algorithmic pricing which combines personalised pricing and dynamic pricing. Although the algorithms are dedicated to collecting non-personal data, a picture of a user's status can largely be built. However, the price is not considered to be personalised, because people with the same status or properties will receive the same offers.[59] With affinity data, an individual is unlikely to be identified, since certain groups of people fall into a particular category,[60] for example in the aforementioned cases in which Uber charges customers with low phone batteries more[61] and Meituan and Didi charge users according to their phone brands.[62] That is to say, iPhone users are assumed to have higher incomes, and to be more willing to pay more than users of cheaper Android phones.[63] In addition, memberships and subscriptions can also be used as criteria to charge people, because platforms sometimes assume that a member or subscriber is more willing to pay, and will set a higher price.[64] The data used to generate pricing cannot help to identify any specific user, but it works well with the status of a group of users, which also exerts a great influence on users.

The benefits of adopting the proposed taxonomy are twofold. Firstly, it follows the way data protection law works, making it easier to analyse each scenario from a legal perspective. Secondly, the classification is consistent both with emerging technologies and the economic

[56] Gerlick and Liozu (n 6); Seele and others (n 6).
[57] Tom Chitty, 'This Is How Airlines Price Tickets' (*CNBC*, 2018): <https://www.cnbc.com/2018/08/03/how-do-airlines-price-seat-tickets.html> accessed 12 November 2021.
[58] 'How Surge Pricing Works | Drive with Uber | Uber' (*Uber*, 2020): <https://www.uber.com/gb/en/drive/driver-app/how-surge-works/> accessed 30 September 2021.
[59] Michele Loi and Markus Christen, 'Two Concepts of Group Privacy' (2020) 33 Philosophy and Technology 207: <https://doi.org/10.1007/s13347-019-00351-0>; Sandra Wachter, 'Affinity Profiling and Discrimination by Association in Online Behavioural Advertising' (2020) 35 Berkeley Technology Law Journal 1: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3388639>.
[60] Wachter (n 59).
[61] Lindsay (n 9); Chowdhry (n 9); Martin (n 9).
[62] Shazeda Ahmed, '"Big Data Swindling"' (*A New AI Lexicon*, 2020): <https://medium.com/a-new-ai-lexicon/a-new-ai-lexicon-81fe13991e31> accessed 12 November 2021; Alexa Lee and others, 'Seven Major Changes in China's Finalized Personal Information Protection Law' (*Stanford University DIGIChina*, 2021) <https://digichina.stanford.edu/work/seven-major-changes-in-chinas-finalized-personal-information-protection-law/> accessed 12 November 2021.
[63] Yu and Goh (n 31).
[64] Ahmed (n 62).

classification of online algorithmic pricing.[65] Thus, the compatibility of the economic classification makes it easier to combine online algorithmic pricing with offline price differentiation, which is conducive to easy analysis.

From the taxonomy above, it is evident that algorithmic pricing suffers more from potential privacy intrusions and unfairness in personal data profiling and affinity data inferences made by sellers, risks which are apparent in relation to the first and the third types. In both of those types, sellers can establish or infer certain sensitive information that users do not intend to reveal, which not only invades the user's private sphere, but also negatively impacts their informational autonomy. In addition, sellers can charge users based on their profiles or inferred sensitive information, which may discriminate against certain groups by imposing unfair conditions on transactions. In the non-personal type, the pricing algorithms mainly use public data to provide prices, which is less detrimental to users' privacy. In fact, pre-internet, price differentiation already existed offline, and should therefore be respected as a legitimate right of sellers in certain circumstances.[66] This leads us to the following discussion of personal data-based and affinity-based online algorithmic pricing in the context of data protection law.

4. The Limited Application of the GDPR to Online Algorithmic Pricing

Generally, algorithmic pricing must trigger the data protection law to protect users' data rights. Although many legal scholars have argued that the GDPR should undoubtedly apply to online algorithmic pricing,[67] this paper argues that affinity-based online algorithmic pricing is highly likely to bypass the GDPR in reality. According to the taxonomy set out above, this paper is dedicated to defining the legal nature of online algorithmic pricing and analysing the level of privacy invasion of online algorithmic pricing which the GDPR is able to cover.

In fact, three types of data are stipulated by the GDPR: personal data, pseudonymous data, and anonymous data.[68] However, the GDPR can only cover personal data and pseudonymous data, while anonymous data is largely ignored.[69] Article 4(1) of the GDPR defines personal data as "(i) any information (ii) relating to (iii) an identified or identifiable natural person",[70] which can be further divided into personal data and pseudonymous data. Although pseudonymous data is still

[65] Townley, Morrison and Yeung (n 5) 6.
[66] Steppe (n 8); Wong (n 8).
[67] Steppe (n 8) 772–775. Zuiderveen Borgesius and Poort (n 7) 356–358.Wong (n 8) 2–3.
[68] Paul Voigt and Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR) A Practical Guide* (Springer International Publishing 2017): <http://link.springer.com/10.1007/978-3-319-57959-7>.
[69] Ibid.
[70] Article 4(1), GDPR.

considered to be personal, additional information is needed to identify the data subjects.[71] Thus, even though it is impossible to identify the data subject directly, the data may still be classified as personal data as long as it can be used to indirectly identify the data subject with additional information.[72]

The first type of algorithmic pricing usually satisfies the definition of personal data, because sellers generally set prices by collecting users' IP address, cookies, and even geo-location data.[73] For example, Amazon uses cookies to analyse customers' behaviours, which translates loyalty to the platform into different bands of prices.[74] In this case, IP addresses, cookies, and other similar data are all recognised as personal data, because they all provide a unique ID that can be used to track data subjects with additional information,[75] as the CJEU acknowledged in the Breyer case.[76] Therefore, it is undoubtedly the case that personal data-based algorithmic pricing based on cookies, IP address, device MAC addresses, and other similar technologies should fall within the scope of the GDPR. However, to clarify the case of affinity-based algorithmic pricing, further discussion is needed from the legal perspective.

4.1. The Operation of Online Algorithmic Pricing Based on Anonymous Data

There are three main reasons why affinity data is unlikely to be considered as personal data, which in turn would mean that the data protection law may not cover affinity-based algorithmic pricing. Firstly, algorithmic pricing can be achieved through entirely anonymous data. Back in 2000, some computer scientists proposed a model capable of inferring users' demographic attributes (e.g. gender, age, or income) from anonymous data.[77] Nowadays, with the progress of technology and the volume of Big Data, more sensitive information can be inferred by algorithms. For example, users' location, age, and other preferences can be inferred only by their mobile communication patterns.[78]

Secondly, instead of directly processing users' personal data for price-making, platforms can build profiles and infer private status (including their social tags and networks, professions, and

[71] Article 4(5), GDPR.
[72] Article 4(5), GDPR
[73] Steppe (n 8); Zuiderveen Borgesius and Poort (n 7).
[74] Ward (n 2).
[75] Recital 30, GDPR.
[76] Case C-582/14, Patrick Breyer v. Bundesrepublik Deutschland [2016] ECLI:EU:C:2016:779.
[77] Dan Murray and Kevan Durrell, 'Inferring Demographic Attributes of Anonymous Internet Users', *International Workshop on Web Usage Analysis and User Profiling* (Springer 2000) 7: <http://link.springer.com/10.1007/3-540-44934-5_1>.
[78] Dong and others (n 21).

preferences) through a context-aware learning algorithm.[79] According to profiles and inferred status, platforms can set prices. Although this approach may need to involve person data processing at some point, more recent legal study reveals that data controllers are increasingly deploying transient data processing technologies that might bypass the GDPR by design.[80]

Thirdly, the algorithm only uses de-identifiable affinity data to infer more private information about the user, which means that individuals cannot be identified, but their information can be revealed. Such technologies can also be used to generate algorithmic pricing. Contrary to Borgesius and Poort's opinion that such processing has limited practical value,[81] more recent studies note that many platforms have deployed such price-making mechanisms, known as "dynamic pricing", which have proved lucrative.[82] For instance, the aforementioned examples of Uber[83] and Meituan both show that there is a close relationship between affinity data and willingness to pay.[84] Instead of identifying a specific individual, the price-making algorithms only categorise users with similar characteristics into a group to charge them a different price from other groups, without building any identity.

However, it is still necessary to scrutinise whether this type of online algorithmic pricing achieves de-identification in the context of GDPR. According to Recital 26 GDPR, all the likely ways of identifying data subjects either directly or indirectly should be accounted for.[85] However, to do so, proportionate effort needs to be considered. For example, having to expend disproportionate time and cost expenditure to identify a particular natural person should not be counted in the abovementioned "all the manners".[86]

Moreover, the Art. 29 WP has issued three criteria to assess whether data is irreversibly de-identified:[87] the ability to **single out** the individual, the ability to **link** to the individual, and the information that can be **inferred** about the individual. In this stipulation, the phrase "single out" refers to the possibility of isolating those records that could be used to identify an individual in the dataset.[88] For example, a unique NHS number combined with additional demographic

[79] Yan Liu, Yangyang Xu and Mei Chen, 'Context-Aware Recommendation System with Anonymous User Profile Learning', *27th International Conference on Software Engineering and Knowledge Engineering* (2015): 1–2 <http://ksiresearchorg.ipage.com/seke/seke15paper/seke15paper_65.pdf>.
[80] Damian George, Kento Reutimann and Aurelia Tamò-Larrieux, 'GDPR Bypass by Design? Transient Processing of Data under the GDPR' (2019) 9 International Data Privacy Law 285, 285–286.
[81] Zuiderveen Borgesius and Poort (n 2) p. 12.
[82] Seele and others (n 6) 704–705.
[83] Lindsay (n 9); Chowdhry (n 9); Martin (n 9).
[84] Yu and Goh (n 31).
[85] Recital 26, GDPR.
[86] Case C-582/14, Patrick Breyer v. Bundesrepublik Deutschland [2016] ECLI:EU:C:2016:779, [46]-[49]
[87] Article 29 Working Party, Opinion 05/2014 on Anonymisation Techniques (WP 216) 0829/14/EN, 3.
[88] Ibid, at 11.

information (such as date of birth) can single out a specific person in the database. Recital 26 GDPR also uses this "single out" capability as a test to measure if an individual can be identified.[89] However, taking a phone's battery information as an example, this is unlikely to isolate a specific person, because many people will simultaneously have the same battery level on the same phone model. Accordingly, the battery information dataset is unlikely to satisfy the definition of "single out". Therefore, if the only pricing condition is the battery level then it is almost impossible to identify or single out the data subject using that data alone. It is also not necessary for successful affinity data-based algorithmic pricing to single out data subjects, but it does allow for personal situations to be inferred, which may cause further discrimination.[90]

Linkability implies the risk that at least two datasets contain information on the same data subjects.[91] In this circumstance, although two records in different databases can be linked to the same individual, it is impossible to single out the individual using either database by itself. Such linkability can, however, render data as personal data. In the context of affinity-based algorithmic pricing, the price is set through a usually broad and vague single condition, which means it is difficult to link to a specific user even if other data is combined with it. For example, as was discussed above, some companies charge more based on users' phone brands,[92] which makes it unlikely that a specific person could be identified simply by linking their phone brand with other data. Additionally, it is difficult to assess linkability because it is unclear what the other data may be capable of when it comes to triggering identification through linkages in the future.[93]

Moreover, inference means the possibility to deduce individual attributes from other sets of attributes with **significant probability**.[94] For example, if the dataset does not directly describe users by their names or other direct identifiers such as their NHS number, but it does describe users by gender, occupation, ethnicity and address, it may still be possible to infer identity-related information.

However, in the context of affinity-based online algorithmic pricing, the information is unlikely to infer users' identities with significant probability. For instance, if phone brand and battery levels are the only available data to determine the price of a taxi journey, that dataset cannot

[89] Recital 26, GDPR.
[90] Mittelstadt (n 19) 479–481.
[91] Ibid.
[92] Yu and Goh (n 31).
[93] Michèle Finck, 'Blockchain and the General Data Protection Regulation: Can Distributed Ledgers Be Squared with Blockchain and the General Data Protection Regulation Law?' [2019] European Parliamentary Research Service 21.
[94] Article 29 Working Party, Opinion 05/2014 on Anonymisation Techniques (WP 216) 0829/14/EN, 12.

infer a concrete identity, because it merely represents a group of users sharing similar tags.[95] Furthermore, affinity data is usually unable to deduce information with significant probability, which means it does not fit the Art. 29 WP definition. If the inference of users' financial situations relies on their phone types and the affordability of their memberships, then it is vague and uncertain. Yet, such an inference is sufficient for online algorithmic pricing, because of the high tolerance of mistakes in this practice.[96] Indeed, the gap between the inferred results and users' real situations does not affect price setting, and such criteria are more likely to conversely cause algorithmic bias and discrimination, widening the possibility (and range of victims) of discriminatory behaviours. However, there is a lack of right and methods for data subjects to guard their legitimate interests against algorithmic bias. Overall, this three-step assessment model is problematic, which can lead to inconsistency with the CJEU's jurisprudence.[97]

4.2. Uncertainty Regarding Personal Data Classification Between the CJEU and Art. 29 WP

Although some affinity data can be anonymous, it remains possible to infer certain conditions or the status of individuals. However, regarding the classification of inference data, there is significant inconsistency between Art. 29 WP and the CJEU. According to Art. 29 WP, the data is likely to impact upon certain personal rights and interests, which means that it should be treated as personal data.[98] In other words, if the data cannot be directly traced back to an identifiable person but can impact upon individuals' rights or interests, then it can be categorised as personal data. In addition, Art. 29 WP contends that personal data includes "subjective" information, opinions, and assessments, which do not need to be proven true.[99] However, the jurisprudence of the CJEU does not support the opinion proposed by Art. 29 WP, which is not legally binding.

---

[95] Linnet Taylor, Luciano Floridi and Bart van der Sloot, *Group Privacy: New Challenges of Data Technologies* (Springer International Publishing 2017); Mann and Matzner (n 10); Mittelstadt (n 19); Loi and Christen (n 59).

[96] Seele and others (n 6).

[97] For example, Cases C-141 & 372/12, YS, M and S v. Minister voor Immigratie, Integratie en Asiel, 2014 E.C.R. I-2081.

[98] Article 29 Data Protection Working Party, Opinion 4/2007 on the Concept of Personal Data, 01248/07/EN WP136, at 8 (June 20, 2007): https://www.clinicalstudydatarequest.com/Documents/Privacy-European-guidance.pdf

[99] Ibid, at 11; See also S Wachter and BD Mittelstadt, 'A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI' (2019) 2 Columbia Business Law Review 443.

In using case *YS, M and S*[100] to assess whether the legal analysis of an immigration application can be treated as personal data,[101] both the court and the Advocate General of the CJEU believed that the data contained in a legal document cannot be regarded as personal data.[102] Thus, the personal data used in the legal analysis is still considered personal, but not the analysis itself. Specifically, the court stated that only "name, date of birth, nationality, gender, ethnicity, religion, and language" can be regarded as personal data; other data derived from personal data should not be considered personal. Accordingly, in the case of affinity-based algorithmic pricing, the analysis or the inferences associated with identified or identifiable individuals cannot be deemed to constitute personal data. As a result, the analysis or inference regarding data subjects falls out of the scope of data protection law, which contradicts the opinion of Art. 29 WP. This is likely to raise uncertainty as to whether affinity data should be regarded as personal data. The practical consequence of such uncertainty is the appearance of deliberately designed GDPR-bypass technologies[103] which mean that online service providers do not process the personal data or de-identify the data subject, but their processing outcomes can still have a negative impact on users.

However, in the later *Nowak* case,[104] the CJEU expressed the opposite view,[105] which was that assessments, comments, and the evaluation of data subjects can impact upon a person's private life, which can be linked to a certain individual. Hence, the data should be categorised as personal data. In the case of an exam, while the answers on the papers, marks earned, and the performance during the exam can all be seen as personal data, the questions on the exam paper are not personal data. Based on the analysis of these two cases, it can be concluded that there is significant uncertainty and inconsistency in the CJEU's judgement of the personal data status of affinity data and inferences.

[100] Cases C-141 & 372/12, YS, M and S v. Minister voor Immigratie, Integratie en Asiel, 2014 E.C.R. I-2081
[101] Although this case is not directly related to algorithmic inference, the legal analysis of the documents can be regarded as analogous to inference, as both involve the assessment of, and forming of assumptions about, the data subject.
[102] Cases C-141 & 372/12, YS, M and S v. Minister voor Immigratie, Integratie en Asiel, 2014 E.C.R. I-2081, [45]–[47].
[103] George, Reutimann and Tamò-Larrieux (n 80).
[104] Case C-434/16, Peter Nowak v. Data Prot. Comm'r, 2017 E.C.R. I-994, [54]–[55];
[105] In this case, an exam candidate, Mr. Nowak, requested to exercise his right of access to his failed exam script. Similarly, the exam script can also be regarded as analogous to algorithmic inference as both involve the evaluation of individuals, although the criteria are different.

4.3. The Limited Remit of the Data Protection Law Regarding Online Algorithmic Pricing

The CJEU's jurisprudence also limits the remit of data protection law. In *European Commission v. Bavarian Lager*, it stipulated that data protection law does not aim to assess the accuracy of the decision-making process that involves personal data.[106] On this basis, the requests of data subjects for access were denied, because their intention was to assess the accuracy of an assessment of personal data.[107] Therefore, in the context of online algorithmic pricing, data subjects actually do not have the right to rectify incorrect inferences based on their data due to the inaccuracy of decision-making algorithms. However, the business model of online algorithmic pricing has sufficient tolerance to accommodate relatively high rates of misclassification.[108] Furthermore, in general, online platforms do not necessarily care whether they accurately categorise their users. This grants data subjects few legal weapons with which to tackle the issue of incorrect algorithmic impressions, which may gradually deepen.

On this basis, the accessibility of data subjects is denied, because assessing the accuracy of personal data inferences is not necessary for the platform involved. Meanwhile, as the ECJ holds in *YS, M and S*,[109] it is sufficient that applicants only need to possess a complete summary of the data in an intelligible form, which allows them to be aware of the data, check its accuracy, and make sure it is processed in compliance with the relevant directive.[110]

In the case of *Nowak*, although the CJEU accepted a broader interpretation of personal data, the total exercise of relevant data protection rights should follow teleological assessment, because the rectification of the answers in the exam is undesirable, and strays from the legislator's intent.[111] Therefore, it concluded that the scope of data protection rights must be interpreted contextually and teleologically regarding the purpose of data collection; thus, the reason for the data collection constrains the remit of data protection law. The Advocate General further illustrated that in addition to reflecting their opinions, the aims of exam markers' comments also serve as a record, where rectification is inappropriate.[112] This means that in affinity-based algorithmic pricing, it is difficult to rectify or delete sellers' inferred data if the data is served as a record. It also implies that the data subject cannot directly exercise their

[106] Case C-28/08 P, European Comm'n v. Bavarian Lager, 2010 E.C.R. I-6055.
[107] Ibid.
[108] Seele and others (n 6).
[109] Cases C–141 & 372/12, YS, M and S v. Minister voor Immigratie, Integratie en Asiel, 2014 E.C.R. I-2081
[110] Wachter and Mittelstadt (n 99) 37.
[111] Case C-434/16, Peter Nowak v. Data Prot. Comm'r, 2017 E.C.R. I-994, Opinion of Advocate General Kokott, 35.
[112] Ibid, 36, 37.

data rights, because they firstly need to assess the purpose of the data collection to evaluate whether the exercise of the data right is teleologically inappropriate. However, appropriateness or otherwise is not defined in the GDPR, causing legal uncertainty.

Furthermore, the Advocate General also pointed out that the remit of data protection law is not to assess the justification behind an assessment or decision,[113] which significantly limits the application of law in protecting personal data against online algorithmic pricing. If the data protection is not designed to evaluate whether the assumptions are accurate, then data subjects might be deprived of the right to correct inaccurate algorithmic decision-making, especially in relation to algorithmic pricing. Therefore, the purpose of processing the personal data will largely influence the data rights of the data subjects.

4.4. Summary

The above analysis demonstrated how the GDPR can regulate personal data-based algorithmic pricing. However, the legal nature of affinity data-based algorithmic pricing is unclear because affinity data cannot be categorised as personal data since it cannot identify a specific user. Thus, while individuals have no control over, or protections against, affinity data-based algorithmic pricing, such price-making mechanisms can nonetheless intrude upon individuals' private lives and digital autonomy, eventually causing discrimination.

Furthermore, there is still no consistent conclusion in Art. 29 WP and the CJEU's jurisprudence regarding the legal nature of inference and affinity data. For example, in the case of *YS, M and S*, the court contended that the data derived from personal data should not be considered personal data. In contrast, in *Nowak*, it was recognised that if the data impacts upon the data subject's private life or can be traced to a specific person, it should be considered personal data. Additionally, the CJEU apparently limits the remit of data protection law, whose aim is not to assess the accuracy of decision-making processes. Regarding the exercise of data rights, the decisions should be analysed teleologically and contextually.

5. Legal Basis of Processing Data for Online Algorithmic Pricing

In discussing the legal basis of online algorithmic pricing,[114] scholars perhaps overlook the fact that price algorithms based on affinity data may not need a legal basis at all, because based on the analysis in section 3, such affinity data is unlikely to be treated as personal data.[115] Accordingly, affinity-based algorithmic pricing does not process personal data; rather, it

[113] Wachter and Mittelstadt (n 99) 44.
[114] Steppe (n 8) 776–781.
[115] Wachter (n 59) 11–17. Wachter and Mittelstadt (n 99) 22–29.

processes data that may have a close relationship with certain statuses or circumstances without the need to identify the user. In this case, the processing could circumvent the mechanism of choosing a legal basis in the GDPR.

Regarding personal data-based algorithmic pricing, the data controller needs to identify at least one of the legal grounds to process personal data. As per Article 6 GDPR, lawful grounds include consent from the data subject, pre-contractual and contractual measures, and the legitimate interests of the controller.[116] Consent from the data subject in the GDPR implies that the consent must be a freely given, specific, informed, and unambiguous indication of the data subject's wishes.[117] Such consent must be specific and explicit to guarantee that the customer is informed. As Steppe has already examined in detail, an overly broad description of data processing to obtain consent is not recognised.[118] Art. 29 WP also suggests that consent should be opt-in for most tracking-based digital market services.[119]

As for pre-contractual and contractual measures as a legal ground, sellers may use these to justify personal data-based algorithmic pricing.[120] However, using this legal ground must satisfy the necessity test, meaning that the seller must prove that using personal data-based algorithmic pricing is vital to entering into a contract. Personal data-based algorithmic pricing as a lucrative but intrusive tool for sellers does not seem strictly necessary to the sales of goods or services, as sellers can set prices in various ways. However, in some special industries personal data-based algorithmic pricing is necessary to provide a quote; for example, an insurance company may use this legal ground to justify certain types of customised insurance.[121] Insurance companies need to know someone's driving habits and accident record in order to assess the potential risk in pricing vehicle insurance for them.[122] Therefore, in order to satisfy the necessity test, the data processing must be relevant, proportionate and necessary, which requires a case-by-case analysis.

In terms of legitimate interest, the right to make a price could form part of the freedom to conduct a business[123] which is enshrined in Article 16 of the European Charter of Fundamental Rights.[124] Moreover, in certain industries, personal data-based pricing and profiling could also

[116] Voigt and von dem Bussche (n 68) 92–95.
[117] Ibid.
[118] Steppe (n 8).
[119] Article 29 Working Party, 'Opinion 03/2013 on Purpose Limitation' (2013).
[120] Voigt and von dem Bussche (n 68).
[121] McGurk (n 55).
[122] Ibid.
[123] Wong (n 8); Steppe (n 8).
[124] Article 16, Charter of Fundamental Rights of the European Union 2012.

improve the sellers' services and systems. For example, European and worldwide institutions have implemented personal data-based algorithmic pricing to improve medicine accessibility as a vital component of the right to the highest attainable standard of health.[125] Therefore, if sellers use legitimate interest as their legal ground, a necessity and balancing test must be carried out in order to assess if such a legitimate interest overrides the interests or fundamental rights and freedoms of the data subjects.[126]

To conclude, affinity-based algorithmic pricing may not need legal ground because of the nature of affinity data in the GDPR. The practice of personal data-based algorithmic pricing could also be lawful if a seller has one of the legal grounds for processing. But, it is worth noting that the GDPR and the guideline issued by Art. 29 WP both stipulate a heavy burden of proof for invoking legitimate interest and pre-contractual and contractual measures as legal grounds, which would normally require a necessity and balancing test. Therefore, it is clear that opt-in consent will be the most widely-used legal ground for the processing of algorithmic pricing. However, whether such a mechanical manner of consent is effective is still doubtful,[127] as the inertia of the data subject means they may simply box-tick without thoroughly examining the terms.[128] Thus, the data rights provided by the GDPR are valuable for data subjects wishing to revoke their consent or object to the processing of their data.

[125] Report of the Special Rapporteur on the right of everyone to the enjoyment of the highest attainable standard of physical and mental health (2008) UN Doc. A/63/263, 23; Steppe (n 8).

[126] The freedom to conduct a business is recognised as one of the fundamental rights enshrined in Article 16 of the EU Charter. In fact, the statement of freedom to conduct a business is very simple, as it simply recognises this freedom without further explanation. According to the CJEU's jurisprudence, *Sky Österreich*, the freedom to conduct a business encompasses the freedom to exercise an economic or commercial activity and the freedom of contract (*see Case C-283/11 Sky Österreich [2013] ECLI:EU:C:2013:28*). Meanwhile, the CJEU also states that freedom of contract entails the freedom to choose business partners and the freedom to set the price for a service (*Ibid; See also Case C-437/04 Commission v Belgium [2007] ECLI:EU:C:2007:178, [2007] ECR I02513, para 51*). Therefore, it is clear that businesses, including online providers of goods or services, have the freedom to set different prices for different customers. This stipulation in the EU Charter may justify the use of online algorithmic pricing, which impedes the exercise of data subjects' rights, especially in relation to affinity-based algorithmic pricing. Following the EU's legal hierarchy, data subjects' rights to protect their personal data and to enjoy their private and family life are equally important as the right and freedom to conduct a business. However, when there are potential conflicts, it is uncertain how to balance these three rights. If the CJEU's jurisprudence is followed, it will render the data protection regime unfeasible against online algorithmic pricing.

[127] Sylvie Delacroix and Neil D Lawrence, 'Bottom-up Data Trusts: Disturbing the "One Size Fits All" Approach to Data Governance' (2019) 9 International Data Privacy Law 236; Zuiderveen Borgesius and Poort (n 7).

[128] L Edwards, *Law, Policy and the Internet* (1st edn., Hart Publishing 2019): <https://books.google.co.uk/books?id=hISzrQEACAAJ>.

6. The Current Limitations of the GDPR Rights Regarding Online Algorithmic Pricing

Regardless of the divergence of views on the status of affinity data, it is necessary to examine whether the current data rights stipulated by the GDPR can effectively protect data subjects against online algorithmic pricing, assuming that affinity data is considered personal data if the *Nowak* decision are followed. Therefore, this section aims to examine rights in the context of online algorithmic pricing. It concludes that GDPR rights are still difficult to protect the legitimate interests of data subjects.

6.1. The Invalid Diverse Data Protection Mechanisms Caused by Exemption

Article 11(2) GDPR establishes an exemption as where the data controller does not identify specific data subjects, Articles 15 to 20 shall not apply unless the data subjects are willing to provide additional information to exercise their right. Such de-identification also requires data controllers to avoid collecting additional information which could be used to identify data subjects.[129] However, from the analysis above, mainstream online algorithmic pricing, namely affinity-based algorithmic pricing, is often used to de-identify a specific user but target a particular customer group created by algorithms; the data controller actually cannot identify a specific individual. Therefore, in most cases, online algorithmic pricing can be exempted from Articles 15 to 20 according to Article 11(2) of the GDPR. In other words, the right to access personal data, the right to rectify and erasure, and the right of portability do not exist for this form of algorithmic pricing, which undermines the several data protection mechanisms set by the GDPR, which fails to protect data subjects against online algorithmic pricing.

The exemption provided by Article 11(2) of the GDPR does not include Article 21 and Article 22. Such frameworks seem mainly to be designed for Automated Decision-Making (ADM) algorithms and profiling. However, the following part discusses the shortcomings of Article 21 and Article 22 when applied to affinity-based algorithmic pricing. Moreover, although Article 11(2) GDPR exempts affinity-based algorithmic pricing, personal data-based algorithmic pricing could still be covered by Articles 15 to 20. The following part explains the difficulties of providing substantial assistance against personal data-based algorithmic pricing via the mechanisms set by Articles 15 to 20 of the GDPR, and discusses the right to know about data processing (Articles 13-15), the right to object (Article 21), and the right not to be subjected to ADM (Article 22). These three mechanisms cannot effectively protect users against both affinity-based and personal data-based algorithmic pricing.

[129] Article 11(1), GDPR

6.2. The Right to Know About Data Processing

The right to know about data processing (Articles 13 to 15 GDPR) intends to establish a transparent environment where data subjects can understand how their personal data is processed and the purpose of data processing.[130] This mechanism is the prerequisite basis for exercising subsequent data protection rights. However, it may not work well for both types of algorithmic pricing.

Article 13 stipulates several obligations for data controllers, which require them to provide data subjects with information about the purpose of data processing and potential third-party recipients. However, the article only covers data directly collected from the data subjects, which means that data derived or inferred from the initial data cannot be covered by the disclosure obligation towards data subjects.[131]

Article 14 covers the personal data obtained indirectly from data subjects, which requires data controllers to provide specific information to data subjects to help eliminate information asymmetry. This information includes the identity and contact details of the controllers, the categories of personal data collected, the intended purposes of the processing, the recipients or categories of third-party recipients, the data controller's or the third party's legitimate interests justifying the processing, and the source of the personal data. Although it is necessary for data controllers to provide all the above information, some loopholes regarding personal data-based algorithmic pricing remain. Firstly, the article only requires data controllers to provide the categories of personal data involved, which are yet to be defined in the GDPR. This indicates that data controllers are not required to disclose the details of the specific processed data.[132] As Wachter and Mittelstadt have argued, a data controller only needs to provide the abstract categories involved, or list types of processed data, leaving data subjects unable to find out which personal data are processed by the controllers to generate a price.[133] Secondly, such information disclosure is not required in situations where the obligation is impossible to fulfil, or disproportionate effort is involved. On the one hand, the GDPR does not clearly define "disproportionate effort", which makes it uncertain in the context of legal enforcement. On the other hand, in the present era of big data every request by a data subject is likely to involve a disproportionate effort from the data controller because specific data needs to be identified from multiple databases. Last but not least, neither Article 13 nor Article 14 creates legal certainty covering the inferred or derived data created by data controllers. In most algorithmic

[130] Voigt and von dem Bussche (n 68).
[131] Wachter and Mittelstadt (n 71) 52.
[132] Ibid.
[133] Wachter (n 59).

pricing cases, data controllers rely on the data derived or inferred from data subjects' personal information to establish customers' profiles. However, in this case, there is no need for data controllers to undertake notification responsibilities.[134]

Although data controllers' notification duties remain uncertain, data subjects' right to access personal data (as per Article 15 GDPR) may be helpful in obtaining the relevant information.[135] According to Art. 29 WP, the right to access applies to inferred and derived data on profiling.[136] However, similar to Articles 13 and 14, Article 15 also states that data controllers need only provide the purposes of the data processing, the categories of personal data, and the source of the data. In order to obtain this information, several additional obstacles arise for data subjects. Firstly, they must fight to discover the identity of the data controllers, which can be challenging in the big data era. Secondly, according to Article 15(3), the exercise of the right to access shall not adversely affect the rights and freedoms of others. Particularly, Recital 63 highlights that exercising the right to access should not adversely impact trade secrets,[137] intellectual property (IP), and notably, the copyright protecting the software.[138] Although controllers cannot refuse to

[134] Wachter and Mittelstadt (n 99).
[135] Article 15, GDPR.
[136] Article 29 Data Protection Working Party, Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679, 17/EN, WP251rev.01, at 17 (2018): http://ec.europa.eu/newsroom/article29/document.cfm?doc_id=49826
[137] The trade secret legislation also hides online algorithmic pricing and increases its opacity. The new Directive on the protection of trade secrets in EU seems to overlook the price algorithms and the relevant data used in setting prices. According to Article 2, trade secrets are defined as any information that is generally not known or readily available in the circles that normally deal with this type of information. Due to its secrecy and scarcity, such information usually has significant commercial value, which is why its owners will take reasonable steps to keep it a secret. Thus, it is clear that price algorithms should fall into this scope, which means that customer profiling data and affinity data (also known as the probabilistic assumption) about customers should agree with this definition. The guideline issues by legislator and the European Data Protection Supervisor (EDPS) have foreseen the potential tension between, but the scope is limited. Recital 34, Recital 35 and Article 9(4) of the new trade secrets law has added that the protection of personal data shall be respected and follow the requirements of the GDPR. However, this is not sufficient in the context of online algorithmic pricing as, for example, affinity-based algorithmic pricing cannot be covered by such a provision because it uses non-personal data to make the price, which harmfully impacts the data subjects. When data subjects want to exercise their rights, the controllers can reject their request claiming trade secrets protection. In terms of personal data-based algorithmic pricing, the data subjects may only be able to access the processing that contains their personal data, However, the accuracy of algorithmic pricing and the model used to calculate the price are still not accessible, which means that customers are likely to be victimised. In particular, the right to rectification may not be exercised in relation to the inferences and probabilistic assumptions made in the algorithms, since it relates to a trade secret. Therefore, further studies of IP law and data protection law are needed to strike the right balance among different rights-holders.
[138] For example, according to the Directive on the legal protection of computer programmes, Article 4(1)(a) stipulates the exclusive right of the rights-holder of a computer programme to permanently or temporarily reproduce that programme by any means, in any form, in part or as a whole. Thus, any kind of reproduction of the computer programme shall be authorised by the rights-holder. The Directive interprets "computer program" broadly. According to Article 1(2), the Directive applies to any form of computer programmes. Accordingly, in the context of online algorithmic pricing, any types of price algorithm should satisfy this definition, which means that when data subjects seek to access their personal data or exercise the right

provide information to data subjects based on the regulation, it greatly weakens the right itself. Moreover, apart from the IP rights, the sellers shall have the right and freedom to conduct their business, formulate contracts, and determine the price of their service.[139]

6.3. The Right of Rectification and the Erasure of Algorithmic Pricing Data

In the context of algorithmic pricing, the rights of rectification and erasure are only marginally useful. Firstly, data subjects must know they have been charged through algorithmic profiling. Secondly, the algorithmic price has to be inaccurate or based on inaccurate personal data. However, from the analysis above regarding the right to know and the right to access personal data, it is clear that data subjects do not have sufficient information to know the type of personal data used in algorithmic pricing. Therefore, huge information asymmetry between data subjects and controllers exists, impeding the exercise of the right to rectify.

Regarding the second premise, if data subjects intend to exercise their rights, the results of algorithmic pricing must be verified as inaccurate. However, it is difficult to prove the inaccuracy of the result of a pricing algorithm because pricing algorithms are generally predictive[140] and subjective.[141] Meanwhile, the price of a service or goods are also subjective and can vary from person to person and from time to time. For example, some people may have a budget of £500 for a smartphone, while others may only have £450 for the same one. In this case, it is hard to verify whether the price algorithm is inaccurate, which means that data subjects are unlikely to use this right against personal data-based algorithmic pricing. Additionally, in most cases algorithmic pricing is accurate, or at least it is based on accurate personal data. Therefore, data subjects cannot exert the right to rectify. In this scenario, it is necessary to examine if data subjects can use the right to erasure and force data controllers to delete the algorithmic pricing profiles.

According to Article 17 of the GDPR, data subjects have the right to erase their personal data if the processing is no longer necessary, or if consent is withdrawn and there is no other legal ground for the processing.[142] This right is also applied when data subjects object to the processing and there are no overriding legitimate grounds for data controllers to continue the processing. Moreover, the right can also be used in the situations where personal data have

---

of rectification and portability, they may need authorisation from the rights-holders. This poses an additional challenge to data subjects.

[139] See footnote 102 for the details.

[140] For example, algorithmic pricing may predict that a customer will have a stable income in next few months.

[141] It is also subjective, as users are often categorised by different tags; for example, high consumption ability with high willingness to pay.

[142] Article 17(1), GDPR.

been unlawfully processed.[143] It is clear that if the data subject intends to use the right to erase, the data controller must not have any other legal grounds for processing or overriding legitimate grounds. Therefore, it is argued that data controllers can deny the erasure request if the data was necessary to the technical development of their algorithms or applications.[144]

Furthermore, as was mentioned above, data controllers can also use their IP rights or cite trade secrets to deny such requests, because the output of algorithms and profiling can be regarded to have commercial value, and therefore usually falls into the category of business secrets. In addition, sellers can also invoke Article 16 of the EU Charter where the freedom to conduct a business is enshrined as a fundamental right.[145] As Malgieri argues, since data controllers significantly invest to build their algorithms, it is hard to delete them at data subjects' request.[146] When data subjects make a request, the financial expenditure involved will surely be considered for the sake of innovation. A potential solution to this dilemma is that data subjects can access or delete the part of data that is strictly related to themselves, while the output of their data processing, as a trade secret, will not be disclosed.[147] In this case, data subjects still cannot rectify or delete the output data of the pricing algorithms Therefore, it is necessary to find a balance between people's right to protect their personal data with sellers' fundamental rights,[148] as the balance is currently uncertain.[149]

Some deem that the right to erasure cannot be applied to algorithms, because it was not designed for that purpose.[150] When it comes to the ADM system, the right to object (Article 21) and the right not to be subject to ADM (Article 22) are more applicable and helpful.[151]

6.4. The Right to Object and not to be Subject to ADM

Since Article 11(2) only exempts Articles 15 to 20 when data controllers cannot identify the specific data subjects, the right to object (Article 21) and the right not to be subject to ADM (Article 22) can cover both types of algorithmic pricing.[152] However, the following discussion

[143] Ibid.
[144] Wachter and Mittelstadt (n 71) 62.
[145] See footnote 102 for the details.
[146] Gianclaudio Malgieri, 'Trade Secrets v Personal Data: A Possible Solution for Balancing Rights' (2016) 6 International Data Privacy Law 102.
[147] Ibid.
[148] Article 8, Charter of Fundamental Rights of the European Union.
[149] See footnote 102 for the details.
[150] Edwards and Veale (n 20).
[151] Gianclaudio Malgieri and Giovanni Comandé, 'Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation' (2017) 7 International Data Privacy Law 243.
[152] If the affinity data is considered to be personal data, then Articles 21 and 22 are able to cover affinity-based algorithmic pricing.

illustrates why the right to object and the right not to be subject to ADM can only provide limited assistance to data subjects against algorithmic pricing.

Article 21 of the GDPR grants data subjects the right to object to data processing, and especially highlights profiling. Unless the controllers can demonstrate "compelling legitimate grounds" for the process that override the rights and the freedom of data subjects, it is necessary for controllers to stop the processing.[153] Meanwhile, the article also underlines that if the processing is for direct marketing purposes, an objection should be granted directly. Therefore, it is apparent that Article 21 is designed as a mechanism to complement the preceding rights, granting data subjects the right to object to profiling and direct online marketing. However, it remains questionable whether such mechanisms can be successfully applied to online algorithmic pricing.

A similar problem associated with the right to erasure also exists in the legal application of Article 21 regarding algorithmic pricing. Article 21 stipulates that controllers' compelling legitimate grounds can provide an exemption from this right. However, a definition of those compelling legitimate grounds is absent. Similarly, the extent to which a legitimate ground can override the right and interests of data subjects remains unclear, which makes it questionable whether the sellers' fundamental right and freedom to conduct their business can constitute the compelling legitimate grounds required.

In addition, although it is undisputed that Article 21 can be applied to direct online marketing, the GDPR lacks a definition of direct marketing. As a result, whether online algorithmic pricing can be seen as a kind of online direct marketing is doubtful. According to the proposed e-Privacy Regulation, Article 4(3)(f) defines direct marketing communications as "any form of advertising, whether written or oral, sent to one or more identified or identifiable end-users of electronic communications services",[154] which narrows down the scope of direct marketing to the advertising level for either identified or identifiable end-users. Accordingly, online algorithmic pricing should not be included in direct marketing, which in turn should not be covered by this Article. Consequently, Article 21 can only provide limited assistance in the context of algorithmic pricing, which means that its regulation of algorithmic pricing still needs further observation.

[153] Article 21(1), GDPR.
[154] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) 2017.

Turning to the right not to be subject to ADM, this right was originally expected to serve as a weapon against algorithms and profiling. However, the right may not work as expected in the context of algorithmic pricing. Firstly, there are two thresholds for applying this right to algorithmic pricing. As is generally argued, the first threshold of applying Article 22 is that decisions must be based solely on automated processing without any evaluation or intervention by other persons, including online profiling.[155] If the personal data is interpreted or assessed prior to the automatic decisions, then the provision may not be applicable because the decision-making will no longer solely involve automatic processing. In order to close this gap, Art. 29 WP issues a guideline declaring that the fabrication of human involvement cannot stop the application of Article 22.[156] Some scholars also argue that most of online algorithmic pricing can satisfy this threshold.[157] However, evidence from computer science research shows that data controllers need to intervene in ADM deployment. For example, after data collection, it often needs human intervention on data cleansing as many of the data collected is dirty.[158] After human assessment of the dataset, data can be used to train the algorithm and make decisions. In this case, human assessment is essential for shaping algorithms and making relevant decisions. As a result, Article 22 is not always applicable to online algorithmic pricing especially when the price decision is not completely based on automatic processing.

The second threshold for applying Article 22 is that the decision must produce legal effects or similarly significant effects regarding data subjects.[159] However, the GDPR does not define legal effect or the similarly significant effect. According to the guideline issues by Art. 29 WP, only serious impactful effects fall into the scope of Article 22(1) of the GDPR.[160] It is argued that although personal data-based pricing can result in legal effects[161], this argument is in fact untenable[162] as it is based on the assumption that algorithmic pricing will indirectly affect data subjects' rights. However, according to Recital 71 of the GDPR, the automatic refusal of an online credit application is considered as a non-legal effect. Secondly, as Wong argues, if legal effects include the indirect altering of data subjects' rights, then this can make demonstrating "similarly significant effects" more impractical, as all decisions can indirectly affect data subjects' rights.

[155] Wong (n 8). Steppe (n 8). Zuiderveen Borgesius and Poort (n 7).
[156] Article 29 Data Protection Working Party, Article 29 Working Party, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679' (2018).
[157] Wong (n 8) 6; Zuiderveen Borgesius and Poort (n 7) 362.
[158] Fakhitah Ridzuan and Wan Mohd Nazmee Wan Zainon, 'A Review on Data Cleansing Methods for Big Data' (2019) 161 Procedia Computer Science 731, 734 <https://doi.org/10.1016/j.procs.2019.11.177>.
[159] Article 22, GDPR.
[160] Article 29 Working Party (n 156).
[161] Steppe (n 8). Zuiderveen Borgesius and Poort (n 7).
[162] Wong (n 8).

Accordingly, legal effects only include the direct legal impact on data subjects. Therefore, algorithmic pricing does not have a legal effect on data subjects.

It is unlikely that algorithmic pricing will similarly and significantly affect data subjects. According to the Art. 29 WP, if the differential pricing sets a prohibitively high price based on personal data or characteristics, it can effectively bar someone from accessing certain goods or services. This will constitute a similarly significantly effect.[163] However, this explanation seems paradoxical. As a marketing strategy open to sellers, algorithmic pricing is unlikely to set prices high enough to prohibitively discourage certain types of customers from buying. Meanwhile, whether a price is high enough to bar someone from certain goods is very subjective and uncertain, as many product prices may stop certain customers from buying them, regardless of whether sellers deploy algorithmic pricing. More importantly, this explanation only targets differential pricing based on "personal data or personal characteristics," which means that it does not cover affinity-based algorithmic pricing. Therefore, from this perspective, these two thresholds impede the application of Article 22 to algorithmic pricing.

However, some scholars have argued that online algorithmic pricing could have a legal/similarly significant effect, and some are indeed based solely on automated processing.[164] Assuming that the first and second thresholds are fulfilled and the application of Article 22 is not impeded, Article 22 still only provides limited protection for users against online algorithmic pricing, for two main reasons. Firstly, Article 22 is still the data subject's right, rather than a legal requirement for the data controller; thus, the data subject must actively exercise this right against online algorithmic pricing. However, the premise of the effective exercise of this right is that the data subject can obtain meaningful information about how their data is processed through the right to know. As previous discussed, affinity-based algorithmic pricing is likely to be exempted from the rights to know and to be informed. Therefore, data subjects will struggle to exercise this right as they may not be aware of online algorithmic pricing. Secondly, the starting point of Article 22 is to require human intervention when there is algorithmic bias.[165] However, as Edwards argues, human involvement can also be rendered nominal by algorithmic bias.[166] Especially in online algorithmic pricing, the data controller deliberately designs the algorithm to maximise their profit, so the utility of human involvement to solve the problem

[163] Article 29 Working Party (n 156).
[164] Alan M Sears, 'The Limits of Online Price Discrimination in Europe' (2020) 21 Columbia Science and Technology Law Review 1, 30–31; Zuiderveen Borgesius and Poort (n 7) 362.
[165] Edwards and Veale (n 20) 44–45.
[166] ibid.

is doubtful. Therefore, as Sears argues, the implementation of additional transparency seems to be key, and further guidance from data protection authorities is required.[167]

Furthermore, the CJEU's jurisprudence may also limit the application of this provision in the context of algorithmic pricing. As was discussed in section 3.3, *European Commission v. Bavarian Lager* ruled that the purpose of data protection law is not to assess the accuracy of decision-making processes involving personal data.[168] Therefore, unless the decision-making standards of algorithmic pricing contain some prohibitive elements, such as violating the anti-discrimination law by using gender, race, or sexual orientation as parameters to set price, it will not fall within the scope of data protection law. This judgement significantly narrows the scope of data protection law, which makes data protection more difficult to achieve for individuals against algorithmic bias. Regarding the anti-discrimination law, Wachter argues that the protected group is established based on historical experience and prior mistakes, including those relating to religions, ethnic groups, and political opinions.[169] However, algorithms create a new kind of group that might quite easily also suffer from discrimination. Unlike the traditional legally protected groups, the discrimination caused by the creation of new algorithmic groups is more concealed, which renders anti-discrimination law nugatory.

To sum up, Articles 21 and 22 of the GDPR seem to be particularly designed for ADM. However, in the context of algorithmic pricing, it is clear that neither of these provisions can provide substantial assistance to data subjects.[170]

7. Potential Solutions

Based on the above analysis, it can be said that two key issues have led the GDPR to lack protection against personal data-based and affinity data-based algorithmic pricing. The first is the legal uncertainty about the classification of personal data. The second is that current data

[167] Sears (n 164) 32–33.
[168] Case C-28/08 P, European Comm'n v. Bavarian Lager, 2010 E.C.R. I-6055.
[169] Frederik J Zuiderveen BorgeWard (n 2).sius, 'Strengthening Legal Protection against Discrimination by Algorithms and Artificial Intelligence' (2020) 24 International Journal of Human Rights 1572: <https://doi.org/10.1080/13642987.2020.1743976>. Borgesius (n 17).Wachter (n 59).
[170] Apart from the GDPR, some place great faith in the Artificial Intelligence Act (AIA) for the regulation of algorithms. However, following the classification of the AIA, online algorithmic pricing is only likely to fall into the limited-risk or minimal-risk AI group. According to Article 52 of the AIA (draft), only transparency obligations are set up for the limited-risk AI system. However, this requirement seems too ambiguous and general. In the context of online algorithmic pricing, the controllers may only inform users with general expressions, such as "the service is provided by an AI system for better customer performance," which is deemed to be sufficient. However, as was previously discussed, a general transparency obligation is apparently insufficient for users to protect themselves against online algorithmic pricing. Additionally, there is debate over the extent to which sellers or platforms should disclose their use of online algorithmic pricing. Therefore, the transparency obligation on sellers or platforms deploying algorithmic pricing is too general and mild, and unlikely to help data subjects suffering from bias.

rights are limited in the protection they offer against affinity data and inferred data. The following part suggests some potential solutions to these two issues.

7.1. Group Privacy as a Tool for the Dynamic Categorisation of Personal Data in ADM

Based on above analysis, one of the main reasons that the GDPR cannot effectively regulate online algorithmic pricing is that it uses identification as a criterion to categorise personal data and non-personal data. This dichotomy neglects the fact that most big data analytics do not need to identify individuals concretely and precisely. In fact, certain inferences drawn from anonymous data and non-personal data, such as affinity data, also pose great risks for data subjects regarding algorithmic pricing. Such risks have already harmed individuals' rights to privacy, quality, and informational self-determination.[171] However, as a prerequisite to triggering data protection law, the matter of identification clearly leaves a gap in the protection of data subjects. As a result, the GDPR is undermined by online algorithmic pricing.

Furthermore, the current dichotomy between personal data and non-personal data ignores another fact, which is that the classification of data in the era of big data and machine learning is dynamic, which means that personal data can be de-identified with diverse technologies and transferred into personal data or exert significant influence on a certain type of individual through big data and machine learning. Therefore, the current binary, static way to categorise data is insufficient, which raises an urgent need for a more dynamic framework.

As has been argued by Mittelstadt, group privacy can serve as a useful tool to overcome this problem, especially in relation to affinity-based algorithmic pricing[172] because the challenge of affinity-based algorithmic pricing is that it is not concerned with a single identified user, but rather it is about a group of users with similar shared characteristics. Group privacy aims to fill this gap to protect collective privacy interests, so a more dynamic classification of data should be considered by combining the group privacy concept. For data which is used for big data analytic purposes, identification cannot be the only prerequisite to trigger the data protection law; instead, a teleological approach and influence-based evaluation should be used. In other words, the criterion for triggering the protection of data protection law should include the collective data and harm to the group of users caused by data processing, in order to protect their collective right to privacy. This means that if the data processing can pose harms to

[171] See Section 2 for a detailed explanation of this point.
[172] Mittelstadt (n 19).

the data subjects or affect their data protection rights or fundamental rights regardless of the identification of single user, then data protection law should be applied.

Furthermore, group privacy also can be a useful tool to realign the remit of the GDPR. As was previously discussed in Section 4.3, the remit of the GDPR is currently limited and inconsistent. Based on the jurisprudence of the CJEU, data protection law should not be used to assess the accuracy of personal data, nor can it be used to assess the justification behind an assessment or decision. However, it can only cover personal data unless other legislation, including anti-discrimination law, is triggered. In terms of the algorithmic pricing, the explanation of data protection law seems to be too narrow to protect individuals against algorithmic bias. As Section 2 discussed, online algorithmic pricing can cause many harms, including infringing individuals' privacy, equality, and private autonomy, and increase information asymmetry. Therefore, to confront invasion of privacy risks, the CJEU and Art. 29WP should realign the remit of data protection law in order protect individuals from online algorithmic pricing.

7.2. Ex-ante Measures to Minimise Harms

As the complete prohibition of algorithmic pricing is not advisable[173] given that not all algorithmic pricing is negative,[174] ex-ante mechanisms should be encouraged to deal with the risks caused by some algorithmic pricing. Sellers may justify the use of a pricing algorithm before it is deployed, and look for any potential ethical and legal risks in advance. Meanwhile, compared to other legislation, including competition law and consumer protection law, one of the advantages of data protection law lies in its ex-ante measures. In comparison to the traditional price differentiation in brick-and-mortar shops, online algorithmic pricing is highly opaque. Therefore, data protection law should help to establish the transparency of algorithmic pricing through an ex-ante mechanism, in order to make algorithmic pricing more pro-competition and pro-consumer.

Regarding data protection law, DPbD and DPIA can be useful tools with which to decrease information asymmetry and establish greater transparency.[175] By taking a risk-based approach, data protection law could require data controllers to justify their reasons for using big data analytics and algorithms, and clearly and specifically show how the price is set by algorithm. If

[173] UK Office of Fair Trading, Coen and Timan (n 12).
[174] Miller (n 8).
[175] Zihao Li, 'Confronting Algorithm Bias Risks : Will Blockchain Provide New Opportunities or Challenges for Data Protection Law?' (2021) 2 Dublin Law and Politics Review 43 <https://heinonline.org/HOL/Page?handle=hein.journals/dublpr2&div=19&g_sent=1&casa_token=&collection=journals>.

the scope of data protection can be expanded, the right to object and the right not to be subject to ADM can be seen as ex-post measures to support ex-ante measures. Thus, there would be two mechanisms to guarantee that individuals have access to enough information about how prices are set, which will help them to choose whether algorithmic pricing or common pricing should be accepted. Such a mechanism could grant data subjects more control over their personal data, thereby returning the autonomy of private decision-making to individuals.

7.3. The Requirement for a Comprehensive Regulatory Approach

As has been discussed by many legal scholars, apart from data protection law, competition law, consumer protection law, and anti-discrimination law are also competent to cover different types of online algorithmic pricing.[176] However, different laws have different focuses when it comes to algorithmic pricing regulation. For example, when gender, age, or other protected group characteristics are used as the basis for pricing, anti-discrimination law has the most power against related infringement.[177] Similarly, competition law may serve better to deal with monopolistic algorithmic pricing and algorithmic collusion. Therefore, a case-by-case analysis is required to regulate online algorithmic pricing, which involves a comprehensive approach combining data protection law, competition law, consumer protection law, e-commerce law and anti-discrimination law. Additionally, it is necessary to strike a balance between different legal systems, and different legislations should take into account the implementation of other legislation, avoiding the problem of one law impeding the implementation of others.

8. Conclusion

To sum up, the analysis above has provided an overview of the concept of online algorithmic pricing in the current EU data protection law before introducing the taxonomy of online algorithmic pricing. At the same time, through the taxonomy, the emergence of affinity-based algorithmic pricing, a new type of algorithmic pricing, has been highlighted. The analysis discovered that the current EU data protection law (GDPR) can only be applied to limited types of online algorithmic pricing, but that it is difficult for it to cover affinity-based algorithmic pricing. Meanwhile, there is further legal uncertainty due to the inconsistency between Art. 29WP and the CJEU in terms of the definition of personal data and the remit of data protection law. This article also examined whether the data rights granted by GDPR can work as expectation in the context of personal data-based and affinity-based algorithmic pricing, and concluded that affinity-based pricing can be exempted from Articles 15 to 20. If the guidance of

[176] Townley, Morrison and Yeung (n 5).Borgesius (n 17).
[177] Inge Graef, 'Algorithms and Fairness: What Role for Competition Law in Targeting Price Discrimination Towards End Consumers?' (2018) 24 Columbia Journal of European Law 1.

Art. 29WP is followed, Articles 15 to 20 can be applied to personal data-based algorithmic pricing. However, due to their broad expression and sophisticated mechanisms, those rights are hardly used by data subjects to protect themselves against personal data-based algorithmic pricing. Regarding the right to object (Article 21) and the right not to be subject to ADM (Article 22), neither of those provisions are able to provide substantial assistance to data subjects in the context of both types of algorithmic pricing. This article also finds that the EU's primary and secondary legislation regarding online algorithmic pricing, including the EU Charter, the IP law, and the trade secret law all pose potential hurdles to the implementation of GDPR. This article finally provided suggestions on group privacy, the remit of data protection law, ex-ante measures, and a more comprehensive regulatory approach.

UK Copyright and Creative Economy Centre
School of Law / University of Glasgow
10 The Square
Glasgow G12 8QQ
www.create.ac.uk

2022/09 DOI: 10.5281/zenodo.6778008

In collaboration with:

University of Glasgow