Frontiers in Business, Economics and Management
ISSN: 2766-824X | Vol. 25, No. 2, 2026

Personalised Pricing and Its Implications for Fairness, Competition, and Privacy

Jiaqi Gao

Beijing New Oriental Foreign Language School at Yangzhou, Yangzhou, 225009, China

Abstract: Personalised pricing uses consumer data to tailor prices to individual willingness to pay. This paper critically examines its implications for distributive fairness, market competition, and privacy through a narrative analysis of economic research and regulatory evidence. Although algorithmic prices could expand access, limited alternatives and unequal digital capabilities can expose vulnerable consumers to disadvantage. Data and algorithmic interaction may diminish competitiveness in particular market contexts; comprehensive profiling raises additional issues with genuine consent and consumer independence. These insights indicate that welfare outcomes depend on market structure and institutional protections, and they advocate collaborative oversight of pricing strategies, data use, and consumer safeguards.

Keywords: Algorithmic Pricing; Consumer Welfare; Data Privacy.

1. Introduction

This essay first challenges the prevailing notion that personalised pricing can achieve a more equitable resource allocation by setting lower product prices for low-income consumers, but argues that it is more likely to impose a heavier financial burden on the disadvantaged groups. Meanwhile, the data and computing resources requirements of personalised pricing may strengthen tech giants' market power, allowing them to reap more consumer surplus and exacerbating wealth concentration. Last, at the societal level, this essay predicts a systemic privacy crisis, ultimately compromising individual autonomy and exposing consumers to long-term security risks.

2. Access Benefits and Their Limits

First, the key mechanism of personalised pricing is to predict the willingness to pay (WTP) of consumers using individual data, thereby setting unique prices for everyone. As income helps to shape WTP, admittedly, this might imply that wealthier consumers will be charged more for the identical product, whereas low-income groups pay less. In this sense, personalized pricing works automatically as an "implicit progressive taxation", and those who are financially constrained can now access goods and services that are unaffordable under uniform pricing.[1] This is especially beneficial in the case of merit goods generating positive consumption externality, like healthcare and education, where personalised pricing expands the consumption for low-income groups and thus is welfare-enhancing. Some companies have already adopted differential pricing by charging lower prices in poorer nations. For instance, in Mexico, such pricing implemented by the pharmaceutical firm Novartis proved to have enhanced the accessibility and affordability of heart failure drugs, helping more patients to receive life-saving treatment.[2]

On the other hand, personalised pricing cannot be entirely regarded as progressive taxation. The real taxation is collected by the government and then redistributed via public spending, but the higher personalised prices paid by wealthy consumers flow to corporations and their shareholders. The above fairness claim becomes even more untenable when noting the fact that personalised prices depend not only on income but also on other factors like product choice and digital skill. Low-income consumers often live in areas with limited product choices and hence have higher WTP. Consequently, they may be charged higher prices than wealthy consumers who face a wider range of alternatives. For example, an investigation targeted to the online pricing of the U.S. firm Staples revealed that areas with higher average incomes of around $59,900 paid discounted prices, while the areas with lower average incomes of around $48,700, which had fewer nearby physical stores and thus less competition, faced generally higher prices.[3] Also, people from more advantaged backgrounds tend to possess stronger digital skills: they are usually better able to understand how algorithms work and use tools like VPNs to avoid tracking, while those from lower-socioeconomic-status backgrounds often lack digital literacy, making them more vulnerable to being harvested by algorithms.[4] Thus, high-socioeconomic-status individuals may obscure consumer profiles, thereby circumventing high prices and obtaining digital privilege.

Moreover, there may be algorithmic discrimination in the context of personalised pricing. When making personalised predictions, algorithms rely on proxy variables that are usually highly correlated with protected characteristics like race.[5] Since such variables often reflect historical inequalities, algorithms can learn from biased data and unintentionally reproduce biases when predicting WTP. For example, U.S. auto insurance companies often use ZIP codes as proxy variables in pricing, but ZIP codes are closely linked to race because of the historical discriminatory redlining policy that exacerbated racial segregation and concentrated minority communities in poorer neighbourhoods.[6] Algorithms encode such historical discrimination into pricing: in Illinois, drivers in minority zip-code areas were charged at least 10% more on average than those in white areas, despite the same realized risks. This demonstrates how algorithms can embed real-world prejudice into personalised prices: disadvantaged consumers may be even charged more due to historical inequalities, ultimately further raising their costs of living.

3. Market Power and Algoritmic Competition

Secondly, the widespread adoption of personalised pricing may further strengthen tech giants' moats, reinforcing a winner-takes-all market landscape. Personalised pricing relies on AI to analyse massive multi-dimensional user behaviour data such as browsing history, purchase records, and location. Overall, the current AI market has already been dominated by a few tech giants like Google and Amazon, who gain significant first-mover advantage in personalised pricing as they have accumulated enormous proprietary data from huge user bases.[7] They further benefit from network effects: more users generate more data, and this improves pricing algorithms, which in turn increases user engagement and generates more data.[8] Beyond data, training and running pricing models requires substantial computing resources, including cloud infrastructure and specialized hardware such as GPUs and TPUs. These resources are already concentrated among tech giants, with Amazon Web Services, Google Cloud and Microsoft Azure together controlling nearly 70% of the global cloud market.[9] And they can spread the high fixed costs across millions of users to achieve economies of scale, while smaller firms face much higher average costs.[10] Consequently, data and computing requirements strengthen the giants' technological moat while imposing significant barriers for small and medium-sized enterprises. So that these giants have the greatest potential to implement personalised pricing: Amazon simultaneously operates online stores as the first-party seller and charges third-party sellers commission fees as the marketplace platform, and Google can monetise data by selling advertisers pricing tools.

Another force weakening competition is algorithmic collusion. Calvano et al. (2020) demonstrate that by continuously monitoring competitors, algorithms can quickly punish any deviation from collusive strategies and reduce the supranormal profit of betrayal, thereby sustaining tacit collusion even without explicit communication.[11] Even if oligopolists have asymmetric cost structures, AI algorithms still spontaneously learn to collude and consistently charge supercompetitive prices. Some may point out regulations to govern anti-monopoly practices. Currently, there are indeed a few regulations, like the European Union's flagship AI Act. But generally, these initiatives have paid little attention to the monopoly threat and prioritized abuse of AI.[12] These regulations could even benefit the established giants, as they have sufficient resources to bear compliance costs. Massimo (2022) estimates the annual compliance costs of around €400,000 to €2 million—a drop in the ocean for giants but imposes insurmountable obstacles for small and medium-sized enterprise who lack resources to meet compliance requirements.[13] What's worse, tacit algorithmic collusion goes beyond the current definition of "anti-competitive practice" because algorithms have no subjective intention to collude, while competitors have no formal agreements.[14] And as algorithms become increasingly complex, algorithmic collusion becomes too covert to be detected.

Therefore, in the era of personalised pricing, people may witness an even more winner-takes-most outcome. Tech giants will possess greater market power, and for each consumer with WTP above marginal cost, they can charge a price nearly equal to the individual's valuation. Consumer surplus will be reaped by giants, shifting wealth further from consumers to them and their shareholders. Using empirical data from the five largest U.S. online retailers, Brown and MacKay (2023) have demonstrated that algorithm-based personalised pricing can raise average prices by approximately 5%, increase firms' profits by 10%, and reduce consumer surplus by 4%, with the largest gains captured by the dominant firms.[15] Conventional wisdom maintains that growing market power brings economies of scale, lowering long-run average costs and ultimately benefiting consumers through lower prices. But this is an illusion in the era of personalised pricing—prices are set based on WTP, not giants' cost structures. Given that personalised pricing is so lucrative, abnormal profits are more likely to be invested in further consolidating data and computing resources or meeting compliance requirements, rather than in product R&D that improves consumer welfare.

4. Privacy and Consumer Autonomy

Finally, the wide use of personalised pricing may trigger a systemic privacy crisis. The crisis may be driven by various parties. For businesses, as the accuracy of personalised pricing depends heavily on the granularity of data, which has become a new factor of production like land, labour and capital, businesses have strong incentives to expand data collection.[16] And it is reported by the Federal Trade Commission (2025) that a wide range of highly personal consumer data, such as mouse movements on webpages or purchase time, has already been used to set individualized prices.[17] For consumers, most cannot effectively protect themselves due to the privacy paradox: their verbal emphasis on the great concern for data privacy often contradicts their actual behaviour.[18] Due to present bias, they tend to exchange sensitive information for immediate gains like minor conveniences and discounts, causing privacy over-disclosure.

The current regulations, such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), are also ineffective in protecting privacy. Assuming consumers are rational decision-makers, policymakers place much of the responsibility for data-sharing decisions on consumers themselves.[19] But corporate privacy policies are often lengthy and obscure. A New York Times analysis found that it took around 18 minutes to read Facebook's privacy policy, and that the privacy policies on nearly 150 popular websites require a legal education or at least a college degree to fully understand.[20] And since the GDPR came into effect, their readability has even deteriorated, as the primary goal of privacy policies is usually to protect companies from potential lawsuits instead of meeting consumers' privacy needs.[21] Due to bounded rationality, the inability to process complex information, consumers often click "agree" without carefully reading the terms and understanding how data will be used. Worse still, privacy choice creates negative externalities because sharing by some consumers affects the payoff of the anonymous.[22] Allowing consumers to decide whether to share data already provides valuable information for businesses, because they can divide consumers into privacy-protecting and data-sharing groups. Then they can inflate the list prices for the former group while offering superficial discounts to the latter. Such a privacy-choice externality implies there will be too much data sharing compared with the social optimum.

Privacy crisis has deeper consequences. Such a data-driven personalised pricing model is essentially built on extracting

both consumer surplus and privacy data. Besides estimating WTP, firms can also use the data to learn consumers' psychological weaknesses and nudge them to make more irrational choices, thereby accelerating the wealth transfer.[23] For individuals, this compromises individual autonomy and dignity, as privacy is the fundamental prerequisite to thinking freely and making autonomous choices. When companies can deeply estimate behavioural patterns and even proactively shape consumption decisions, there will be no "free choice"—people are essentially making "choices" within the scope of algorithmic manipulation. Moreover, as large-scale data is a valuable target for hackers, there might be substantially higher risks of data breaches. Currently, there are already over 1,700 posts per month on average on the dark web that are intended to trade corporate databases, including identity information, financial details, and trade secrets.[24] So in the era of personalised pricing, consumers are not just exposing themselves to firms but are also confronted with a long-term systemic security risk: once a database is breached, they will face a chain reaction of severe consequences like identity theft and financial fraud.

5. Discussion and Practical Implications

In summary, this essay holds a pessimistic view of personalised pricing. Technology can actually amplify the real-life socioeconomic inequalities. The prevailing notion that personalised pricing benefits the poor by offering them lower prices is too optimistic. Rather, high-socioeconomic-status individuals may obtain digital privilege as they usually possess more product choices and stronger digital skills, and algorithms may proxy historical prejudice into the personalised pricing models. Additionally, the data and computing resources requirements mean tech giants can consolidate market dominance and reinforce a winner-takes-all landscape. This essay's prediction of a privacy crisis implies the erosion of individual autonomy and security. Therefore, if personalised pricing came to be widely used in the future, society should carefully consider the above issues of fairness, competition, and privacy, so as to prevent technology from ultimately becoming an accelerator of structural inequality and digital vulnerability.

References

[1] Krishna, A. (2025). In defense of "surveillance pricing": Why personalized prices could be an unexpected force for equity. The Conversation. https://doi.org/10.64628/aai.j346j39ar

[2] Global Pricing Innovations. (2025, December 17). Bridging the gap: Pharmaceutical pricing and the urgent need for equitable access to medicines in low- and middle-income countries. https://globalpricing.com/bridging-the-gap-pharmaceutical-pricing-and-the-urgent-need-for-equitable-access-to-medicines-in-low-and-middle-income-countries/

[3] Valentino-DeVries, J., Singer-Vine, J., & Soltani, A. (2012, December 24). Websites vary prices, deals based on users' information. The Wall Street Journal. https://www.wsj.com/articles/SB10001424127887323777204578189391813881534

[4] Sáez-Linero, C., Rodríguez-de-Dios, I., & Jiménez-Morales, M. (2026). Algorithmic personalization and social inequality: Young people's knowledge and perceptions of bias in digital advertising. Technology in Society, 86, 103287. https://doi.org/10.1016/j.techsoc.2026.103287

[5] Tschantz, M. C. (2022). What is proxy discrimination? In 2022 ACM Conference on Fairness, Accountability, and Transparency. https://doi.org/10.1145/3531146.3533242

[6] Angwin, J., Larson, J., Kirchner, L., & Mattu, S. (2017, April 5). Minority neighborhoods pay higher car insurance premiums than white areas with the same risk. ProPublica. https://www.propublica.org/article/minority-neighborhoods-higher-car-insurance-premiums-white-areas-same-risk

[7] Bandama, R. (2025, November 28). How Big Tech's monopoly of AI threatens fair competition. TRENDS Research & Advisory. https://trendsresearch.org/insight/how-big-techs-monopoly-of-ai-threatens-fair-competition/?srsltid=AfmBOooI9WVf2m_-wqu2c_xuS6Wp-lo77_hAb5Xo-RZple1D9lHhxaVD

[8] Yborra, M. (2026, March 11). What is a MOAT? Understanding its application in the tech industry. Vaultinum. https://vaultinum.com/blog/moat-in-tech-industry

[9] May, R. (2024). Artificial intelligence, data and competition. OECD.

[10] Adams, J. J., Fang, M., Liu, Z., & Wang, Y. (2025). The rise of AI pricing: Trends, driving forces, and implications for firm performance. Journal of Monetary Economics, 157, 103875. https://doi.org/10.1016/j.jmoneco.2025.103875

[11] Calvano, E., Calzolari, G., Denicolò, V., & Pastorello, S. (2020). Artificial intelligence, algorithmic pricing, and collusion. American Economic Review, 110(10), 3267–3297. https://doi.org/10.1257/aer.20190623

[12] von Thun, M. (2023, October 23). Monopoly power is the elephant in the room in the AI debate. TechPolicy.Press. https://www.techpolicy.press/monopoly-power-is-the-elephant-in-the-room-in-the-ai-debate/

[13] Massimo, M. (2022, December 5). The AI Act: Help or hindrance for SMEs? European DIGITAL SME Alliance. https://www.digitalsme.eu/the-ai-act-help-or-hindrance-for-smes/

[14] Ezrachi, A., & Stucke, M. E. (2016). Virtual competition: The promise and perils of the algorithm-driven economy. Harvard University Press.

[15] Brown, Z. Y., & MacKay, A. (2023). Competition in pricing algorithms. American Economic Journal: Microeconomics, 15(2), 109–156. https://doi.org/10.1257/mic.20210158

[16] Chen, Q. (2022, February 9). China wants to put data to work as an economic resource—But how? DigiChina. https://digichina.stanford.edu/work/china-wants-to-put-data-to-work-as-an-economic-resource-but-how/

[17] Federal Trade Commission. (2025, January 17). FTC surveillance pricing study indicates wide range of personal data used to set individualized consumer prices. https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-surveillance-pricing-study-indicates-wide-range-personal-data-used-set-individualized-consumer

[18] Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision making. IEEE Security and Privacy Magazine, 3(1), 24–30. https://doi.org/10.1109/msp.2005.22

[19] Li, X., Li, B., & Yang, Z. (2024). The dark side of voluntary data sharing. MIS Quarterly. https://doi.org/10.25300/misq/2024/18829

[20] Litman-Navarro, K. (2019, June 12). We read 150 privacy policies. They were an incomprehensible disaster. The New York Times. https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html

[21] Dorfleitner, G., Hornuf, L., & Kreppmeier, J. (2021, October 28). Promise not fulfilled: FinTech, data privacy, and the

GDPR. SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3950094

[22] Rhodes, A., & Zhou, J. (2024). Personalization and privacy choice. The RAND Journal of Economics.

[23] Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. Journal of Information Technology, 30(1), 75–89. https://doi.org/10.1057/jit.2015.5

[24] Kaspersky. (2023, December 12). Average 1,700 posts with corporate data surface on the dark web monthly. https://www.kaspersky.com/about/press-releases/average-1700-posts-with-corporate-data-surface-on-the-dark-web-monthly