Philosophy and Social Science Vol. 3 No. 5, 2026

A Study on the Protection of Consumer Information Rights in "Big Data Price Discrimination"

Zhang Mengxue
School of Political Science and Law, University of Jinan, Jinan, China

Abstract: Online shopping and various service platforms have become deeply embedded in people's daily lives, thanks to the rise of the internet big data era. However, some providers, while offering tailored services, have been caught illegally gathering and abusing personal data from consumers, going so far as to engage in what's known as big data price discrimination. Such actions clearly undermine the principle of fair play in the marketplace and do real harm to consumers' legitimate rights and interests. Within China's academic circles, there's an ongoing debate about how to legally define this practice. Most scholars tend to see it as a form of price discrimination, but a minority argues that it amounts to price fraud. China has put in place a legal framework that takes the Civil Code as its foundation, the Personal Information Protection Law as its centerpiece, and various specialized regulations to fill out the system. Even so, many practical problems persist. To tackle these issues, we could look at tightening up the notice and consent rules for businesses, fine-tuning the antitrust laws, beefing up the mechanisms that protect consumer rights, and making greater use of public interest litigation, all in order to raise the level of protection and ensure fairer market conditions.

Keywords: Big Data Price Discrimination; Price Discrimination; Price Fraud; Consumer Rights

1. How to Define Big Data Price Discrimination

Big data price discrimination is also called personalized pricing. Here's how it works: to maximize profits, some platforms collect user information. They use big data algorithms and take advantage of the information gap between consumers and businesses. Based on consumers' different buying habits, they set different prices for the same product or service. And these price differences have nothing to do with costs.

In Chinese academic circles, the prevailing view characterizes big data price discrimination as a form of price discrimination. Scholars such as Gao Fuping and Wang Yuan argue that while this practice fits the conceptual features of price discrimination, it still violates the provisions on differentiated pricing in China's Price Law and the Law on the Protection of Consumer Rights and Interests. Zheng Zhihang and Xu Zhaoxi see it as a typical form of covert algorithmic discrimination in the era of big data, with price discrimination and targeted promotions being merely two common manifestations of such algorithmic discrimination. Scholars like Wang Xueting and Sun Xiaoya approach the issue from a different angle. Based on its impact on consumer behavior and customer loyalty, they characterize the practice as price deception. Liu Jiaming, by contrast, places greater emphasis on the subjective intent of businesses. In his view, it constitutes price fraud - a deliberate act by merchants that goes against the genuine will of consumers.

1.1 What Is Price Discrimination

Price discrimination centers on adopting varied pricing schemes for nearly identical products and services across diverse customer groups. Its definition and interpretation vary noticeably when viewed from economic and legal perspectives. Economists usually divide such practices into three categories. First-degree discrimination charges prices according to each buyer's personal willingness to spend.Second-degree discrimination adjusts fees depending on buying quantities. Third-degree discrimination separates prices by distinct consumer group traits. Many researchers hold that personalized big-data pricing for loyal users falls into first-degree price discrimination. Different from the other two types, this form heavily depends on massive gathering and accurate analysis of personal consumer data.

The legal field, nevertheless, does not have a

clear and formal definition of price discrimination. Relevant disputes including personalized charging and algorithm-driven monopoly, which belong to big data price discrimination, are mainly regulated by China's Anti-Monopoly Law, Price Law and other related regulatory rules. As stated in Article 9 and Article 22 of the Anti-Monopoly Law, business entities are forbidden from carrying out illegal monopolistic acts through data, algorithms, technologies, capital strength or platform mechanisms. Meanwhile, firms holding dominant market shares cannot abuse their status via the same digital advantages. Taken together, these clauses only lay general restrictive requirements for corporate algorithm use. They fail to clarify detailed features of algorithmic monopoly behaviors, nor specify legal liabilities caused by violation of these rules.Furthermore, the Provisions on Prohibiting the Abuse of Market Dominance provide a detailed interpretation of the provisions on the abuse of market dominance in the Anti-Monopoly Law, Article 19 defines transaction counterparts under the same conditions and lists four scenarios of differential treatment; however, the interpretation regarding digital platform enterprises' abuse of market dominance through data, algorithms, technology, and platform rules remains a mere repetition of Article 22 of the Anti-Monopoly Law. Furthermore, Paragraph 5 of Article 14 in the Price Law clearly states that business operators must not practice price discrimination against other counterparts when offering the same goods or services under equal transaction terms. This rule only sets a basic standard for fair pricing among business entities. It does not extend the ban on price discrimination to cover individual consumers.

1.2 The Theory of Price Fraud

When it comes to defining big data price discrimination, most scholars classify it as a form of price discrimination. Yet a number of Chinese academics hold a different view. They argue that such behavior should be recognized as price fraud. Rooted in moral philosophy and the principle of distributive justice, this view points out that even platforms without a dominant market position can use algorithms to collect consumer data, build user profiles, and charge different prices. These practices raise serious risks, including unfair competition and tacit collusion. They also take too much consumer surplus and violate consumers' legitimate rights and interests. For these reasons, such acts fit the legal elements of price fraud.

According to Article 14, Paragraph 4 of the Price Law and Article 2 of the Provisions on Clear Price Marking and Prohibition of Price Fraud, price fraud refers to business operators using false or misleading pricing methods to induce transactions. Its scope of application covers transactions between business operators and consumers, making it more inclusive than price discrimination. The elements of this offense require the business operator to act with subjective intent, using inducement or deception to act against the consumer's true will, thereby harming their expected benefits and right to fair transactions. Such behavior rapidly erodes market trust, affects business cooperation and financing, reduces the efficiency of resource allocation, and creates a vicious cycle.Furthermore, big data price discrimination infringes upon consumers' right to information by concealing the fact of tailored pricing for each individual. Article 20 of the Consumer Rights Protection Law and Article 9 of its Implementing Regulations both stipulate that businesses bear a duty to provide comprehensive and truthful information and must not set differential prices without the consumer's knowledge. However, by remaining silent about the existence of personalized pricing despite being fully aware of it-in an effort to maintain user trust-platforms have already infringed upon consumers' rights to information and fair transactions.

Nevertheless, there remains controversy over whether big data price discrimination should be fully characterized as price fraud. The core difficulty lies in determining the business operator's subjective intent to defraud. Currently, most merchants on these platforms have fulfilled their basic information disclosure obligations. Relying solely on price discrepancies, without direct evidence of bait-and-switch tactics or misleading advertising, makes it difficult to logically and rigorously infer fraudulent intent under the law. In light of the evolution of algorithmic technology, the author believes that the regulation of big data price discrimination should return to the realm of consumer personal information protection to promote the fair operation of market transaction rules.

2. Current Status and Challenges of

Legislation on the Protection of Consumers' Personal Information Rights in China

2.1 Current Status of Legislation on the Protection of Consumers' Personal Information Rights

When you look at how China protects consumers' personal information through legislation, you see a system that's pretty layered and works from a bunch of different angles. At the heart of this legal framework is the Civil Code, which acts like the foundation, with the Personal Information Protection Law sitting right at the center. Then you've got other specialized laws like the Consumer Rights Protection Law and the E-Commerce Law playing a supporting role, and on top of all that, there are industry standards and various judicial policies adding further details. To be specific, Article 111 of the Civil Code really broke new ground by recognizing the right to personal information as a standalone type of personality right, which laid the groundwork for protection under civil law. The Personal Information Protection Law then goes a step further by spelling out the rules for how data should be handled, and it works hand-in-hand with the Civil Code to create this joint regulatory setup, one that mixes public and private law. That's how we get an institutional path forward for actually making consumers' information rights a reality.

Consumer personal information rights differ fundamentally from general personal information rights in three key dimensions. For legislative goals, the former aims to stabilize market operation and sustain consumer trust, functioning as an economic regulatory tool; the latter prioritizes safeguarding personal dignity and balances the application of public and private legal norms. When it comes to applicable scope, consumer-related information rights only cover data generated amid consumption activities, whereas general personal information protection applies to all data linked to natural persons. In terms of legal nature, consumer information rights carry dual personality and property attributes centering on users' control over private data; general personal information protection counts as a specific human right built upon informational self-determination and guarantees individuals' overall dominion over their own personal data.

2.2 Dilemmas in Protecting Consumers' Personal Information Rights in Big Data Price Discrimination

The preceding paragraphs sort out China's current legal arrangements for consumer personal information protection. Chinese lawmakers protect relevant interests from both public and private legal dimensions, and relevant protection principles have been embedded into formal laws, administrative regulations and industrial codes. Nevertheless, real-world protection still encounters multiple practical hurdles waiting to be sorted out properly, particularly against the backdrop of big data-driven differential pricing.

1. Obstacles Arising from the Civil Code and Personal Information Protection Law

So, these two laws set up what's called the notice and consent rule. Basically, before any data processor can collect or use personal info, they have to fully tell the user what's going on and get their clear permission. But here's the problem: this whole setup runs into a pretty big structural issue in the big data age. Because a lot of personal data is kind of out there in the open, it's really hard for users to keep control over it every step of the way. And on top of that, the law uses the same standard of consent for both the initial collection of data and any later, secondary use of that data. That means users end up losing real control once their data starts moving around. Take big data price discrimination as an example. The platform might tick all the boxes for notice and consent when it first collects the data, but once the algorithms get to work analyzing it, or when the company wants to develop new uses for that data, the user has no way to give ongoing permission. What's even more striking is how most platforms use these blanket consent terms buried in their standard contracts, which basically force users to say yes to long, confusing privacy policies. People can't really understand the details of what'll happen to their data, so how can they give separate or dynamic consent when it comes to sensitive information? In the end, the rights that the law supposedly gives them become nothing more than empty words on paper.

2. Deficiencies Existing in the Anti-Monopoly Law

Under Article 22 of the Anti-Monopoly Law, those operators who hold a dominant spot in the market aren't allowed to engage in discriminatory treatment of their customers. But

when you try to apply this rule specifically to big data price discrimination, you run into three pretty clear problems. One issue is that the standards we use to figure out who actually has a dominant market position are kind of outdated. Yes, the 2022 version of the law added some language about using algorithmic advantages to pull off monopolistic acts, but even so, courts and regulators still have to do a lot of piecing together by referring to the Guidelines on Anti-Monopoly in the Platform Economy Sector to make a final call, which brings a lot of uncertainty into judicial practice. Another problem is that it's extremely tough to determine what counts as equal terms of transaction. Prices get pushed around by all sorts of dynamic factors, so platform operators often point to the various individual differences among consumers as a way to argue that their transaction conditions aren't really the same across the board, and that lets them dodge being accused of differential treatment. There's also a third limitation, which has to do with the regulatory focus being in the wrong place. You see, the Anti-Monopoly Law is mostly concerned with

3. The Dilemma of the Consumer Rights Protection Law

Article 20, Paragraph 3 of the Consumer Rights Protection Law says that operators have a duty to make their prices clear, and Article 55, Paragraph 1 lays out the rules for punitive damages. But when you put this law up against big data price discrimination, it just doesn't do a very good job of stopping it. If you take a narrow reading of the law, as long as the operator puts a price tag on a product, that's pretty much considered enough to satisfy the clear-pricing obligation, and charging different people different prices isn't itself seen as violating that duty. On top of that, because the algorithms companies use might be protected as trade secrets, consumers have a really hard time figuring out why they're seeing one price instead of another. And here's the bigger problem: based on what Article 14 of the Price Law and Article 3 of the Provisions on the Prohibition of Price Fraud say, it's very hard to classify big data price discrimination as price fraud. That means the punitive damages rule just can't be applied here. As things stand now, there's no explicit prohibition in the law that stops online platforms from using algorithmic systems to build highly detailed consumer profiles and then charge different prices to different groups of people.

4. Why Individual Consumers Have a Hard Time Seeking Legal Remedies for Information Rights Violations

For a consumer to legally get compensation, you first have to be able to classify what the platform operator did as an actual infringement. But when you're dealing with big data price discrimination, consumers run into a bunch of obstacles if they try to seek legal remedies. For one thing, the burden of proof placed on them is really high. The standard contract clauses buried inside platform privacy policies, plus the general lack of transparency about how consumer information gets used, make it very difficult for an individual to prove that there's a cause-and-effect link between the actual harm they suffered and what the operator did. Another obstacle is that the economic harm is really tough to put a number on. A consumer can't just point to the price difference between what they paid and what some other user paid, and claim that difference as their actual loss, which means they can't meet the evidentiary standard needed for a damages claim in court. And then there's the issue with punitive damages. Because big data price discrimination is so hard to classify as price fraud under current law, the punitive damages rule in Article 55 of the Consumer Rights Protection Law just doesn't apply to these kinds of disputes.

3. Pathways for Protecting Consumers' Right to Information in the Context of "Big Data Price Discrimination"

3.1 Getting Businesses to Follow the Notice-Consent Rules

The whole notice-consent system really depends on businesses doing a good job of telling people what's happening with their data but they can't. So to stop it from happening, we really need to raise the bar for how businesses handle this duty to inform.For one thing, the rules about what counts as proper disclosure should be tightened up. The law could require businesses to use clearer, easier-to-understand methods, like breaking info down into different levels or using pictures and charts, so consumers actually get what's going on with their data. Breaking it down by level usually means splitting things into three tiers based on how sensitive the info is-a basic version, a more detailed one, and a technical deep-dive for the truly curious. Using visuals, like charts or animations, makes the key

points way easier to take in. Regulators should also set up a system to really check whether disclosures are up to scratch, like coming up with a standard template for everyone to use and doing surprise spot checks now and then. Another idea is to add an instant notification feature that pops up a reminder whenever a user does something that might involve their data, which would make the whole disclosure process much more timely and on point.

3.2 Relaxing Restrictions on the Subjects of Discrimination

When you look at today's platform economy, you'll notice that even those operators who don't have a dominant position in the market can still pull off algorithmic price discrimination, just by making use of the data resources they have access to. That means our traditional way of identifying who qualifies as a subject of price discrimination just isn't good enough anymore. So we really need to loosen up those subject restrictions found in the Anti-Monopoly Law. Instead of only going after dominant platforms, the scope of regulation should be expanded to also cover those non-dominant ones that manage to exert a lot of influence simply because of their data advantages.

Two major adjustments can be implemented in regulatory and judicial practices. Authorities should reconstruct the evaluation standards for market dominance. Rather than overemphasizing rigid market share figures, regulators shall conduct comprehensive assessments that take data processing capabilities, network effect scale, economic scale benefits and user stickiness into full account. Second, introduce the theory of relative dominance to include platforms that, while not holding a dominant market position, possess a significant advantage over consumers in specific scenarios within the scope of regulation, Reference can be made to Article 35 of the E-Commerce Law and the experience outlined in Japan's Antitrust Guidelines on the Abuse of Relative Superiority by Data Platform Companies in Transactions with Consumers.

3.3 Improving Consumers' Right of Withdrawal

In the phenomenon of big data price discrimination, operators, through in-depth processing of user data, disrupt established transaction norms. Their differential pricing strategies clearly violate consumers' basic expectations of price transparency and constitute a deliberate breach of traditional commercial ethics. Article 20 of the Consumer Rights Protection Law and the principle of good faith both require operators to fulfill their duty to inform; when operators conceal important information to implement differential pricing, this essentially constitutes passive fraud.

The consumer's right of withdrawal aims to address issues of information asymmetry and lack of genuine consent in consumer contracts. From a legal perspective, big data price discrimination should be brought under the scope of Article 25 of the Consumer Rights Protection Law: in cases where physical returns are feasible, consumers should be guaranteed the right to return or exchange goods without cause; in cases where returns are not feasible, if the business operator has failed to fulfill its duty to inform, this should be deemed passive fraud and regulated under Article 55. At the same time, legislative efforts should standardize the definition of price fraud, systematically clarify the boundaries between promotional activities and price fraud, and revise the practice of using original price as the sole basis for judgment. For improper pricing practices implemented by operators using big data technology, investigations and penalties can be imposed directly under relevant provisions, without excessive focus on whether such practices should be characterized as price fraud.

3.4 Strengthening Public Interest Litigation for the Protection of Consumer Personal Information

Due to the covert and dispersed nature of big data price discrimination and the widespread harm it causes to legal interests, coupled with the significant disparity in bargaining power between consumers and platforms, private litigation has proven ineffective in protecting consumer rights. Article 70 of the Personal Information Protection Law incorporates personal information protection into the scope of public interest litigation, with filing criteria including: the existence of illegal processing of personal information, and such conduct infringing upon the rights of numerous individuals.

The determination of the illegality of big data price discrimination should not be limited to the result of discriminatory pricing alone; rather, it should examine every stage of the formation

process-from the lack of informed consent during data collection and the opacity of the data analysis process to the imbalance of rights during data circulation-all of which constitute illegal acts and fully meet the prerequisites for initiating a public interest lawsuit. Regarding the requirement of infringement upon the rights and interests of a large number of individuals," the interpretation of infringement should not be limited to actual harm; as long as "price discrimination against loyal customers occurs, the risk of infringement should be deemed to have already materialized. The definition of a large number should also focus on the potential harm to an unspecified majority of the population or to the public interest, rather than being understood solely in terms of the number of consumers.

References

[1]He Haoyang. Platform Private Power Behind Big Data Price Discrimination and Its Legal Correction [J]. Journal of Chongqing University (Social Sciences Edition), 2023, 29(06): 220-232

[2]Luo Jingwei. Challenges and Governance Strategies for Consumer Rights Protection in the Digital Economy: An Analysis of Regulatory Pathways for Algorithm-Based Infringements on Consumer Rights [J]. Price Theory and Practice, 2023, (02): 32-35.

[3]Zhao Danyang. On the Pathways to Establishing Consumer Rights Protection under Algorithmic Price Discrimination [J]. Price Theory and Practice, 2024, (11): 81-87.