Research on the Mechanism and Dynamic Trade-Offs of the Personal Information Protection Law on Marketing Compliance and Performance of Small and Medium-Sized Internet Enterprises under Digital Economy Governance

Mandi Yang, Zhen Han
Sias University, Zhengzhou, Henan, China

Abstract: This study investigates the practical effects of the Personal Information Protection Law (PIPL) on small and medium-sized internet enterprises (SMIEs) in the context of digital economy governance. By constructing an interactive model that combines compliance pressure, resource constraints, and adaptive strategies, and conducting dynamic equilibrium analysis, this paper analyzes how legal regulation transforms corporate marketing practices, and how these transformations jointly affect operating costs, user trust, and innovation. The results show that corporate performance presents a non-linear trend, characterized by significant short-term pressure and long-term differentiation. The core mechanism lies in whether enterprises can effectively translate external compliance requirements into internal management practices, and achieve dynamic balance among cost control, trust building, and innovation incentives. The study suggests that enterprises should reposition compliance from a passive cost burden to an active strategic resource. With targeted resource allocation, the application of privacy-enhancing technologies, and the construction of collaborative networks, SMIEs can enhance business resilience and build sustainable competitive advantages under regulatory requirements.

Keywords: **Personal Information Protection Law; Marketing Compliance; Performance Trade-Offs; Adaptive Strategies; Privacy-Enhancing Technologies**

1. Introduction

As the digital economy expands rapidly, data has become a core factor of production, yet it has also given rise to unprecedented conflicts between personal privacy protection and business data application. In this context, China's Personal Information Protection Law has set up a complete legal system for regulating data processing activities. For small and medium-sized internet enterprises that depend heavily on user data for business operations, the law's rigorous compliance rules have brought far-reaching effects on their daily operation and development. This paper focuses on the marketing compliance adjustments made by such enterprises after the law took effect. It explores the complex relationship between compliance practices and corporate short-term and long-term performance, as well as the dynamic trade-offs enterprises must make among compliance costs, innovation motivation, and market competitiveness. The research is intended to provide both theoretical support and practical references for optimizing the digital economy governance system and promoting the sustainable development of internet enterprises.

2. Theoretical Foundation and Institutional Context

2.1 Theoretical Framework and Core Themes of Digital Economy Governance

Digital economy governance is a normative response to the profound economic and social restructuring brought by digital technologies. Its core task is to design rules, institutions and mechanisms to coordinate the circulation, utilization and allocation of data rights, so as to strike a balance among innovation incentives, fair competition and individual rights protection. Traditional market failure theory offers a basic analytical perspective: the natural monopoly trend in digital markets, the negative externalities caused by data abuse, and the security risks of personal information all provide rationales for regulatory intervention. Governance theory further underscores

multi-stakeholder participation, shifting regulatory responsibility from governments alone to platforms, industry associations and individual users.

Major governance concerns cover the definition of data property rights, algorithm accountability, and cross-border data flow regulation. For small and medium-sized internet enterprises, these macro-level governance issues are directly reflected in daily operations. Strict data protection rules may increase compliance costs and restrict innovation space, but regulations that restrict the anti-competitive practices of large platforms also help create a more level competitive environment. Therefore, grasping the overall context of digital economy governance is a necessary foundation for examining how specific legal provisions influence the behavior and performance of micro-enterprises [1].

2.2 Core Provisions of the Personal Information Protection Law and Regulatory Focus on Marketing

As a key law protecting personal information in China, the PIPL centers on three core rules: clear notice and genuine consent, collecting only what's necessary, and full legal responsibilities for anyone handling user data. Together, these rules set the main boundaries for internet marketing.

First, the notice-consent rule requires companies to openly explain what data they collect, how they use it, and for what purposes—using plain language that users can easily understand. They must get separate, voluntary permission before building user profiles, sending personalized suggestions, or running targeted ads. This ends the old practice of hidden agreements or pre-checked boxes, making data-driven marketing more transparent and respectful to users.

Second, the necessity and minimization rule bans unnecessary data collection. Companies can only collect data that directly relates to their marketing activities, with clear and reasonable goals. This stops wide-ranging, unrestricted collection of user behavior data and pushes marketing to become more focused and scenario-based.

Third, the law sets rules for automated decisions, such as algorithm-based pushes using user profiles. It requires these systems to be open, fair, and non-discriminatory, and users must be able to opt out or choose non-personalized versions. This limits over-reliance on algorithms in marketing and helps strike a better balance between efficiency, fairness, personalization, and user control.

Overall, the PIPL puts strict legal limits on how marketing uses personal data, emphasizing lawful collection, controlled processing, and accountable algorithm use. It has completely changed the standards and ways companies handle marketing compliance [2].

3. Compliance Adjustments and Performance Linkages

3.1 Drivers and Manifestations of Marketing Compliance among SMIEs

Small and medium internet companies don't adjust their marketing compliance on a whim-there are several real pressures pushing them to act.The biggest and most non-negotiable reason is the strict rules and heavy penalties in the PIPL. The law sets hard lines they can't cross. Beyond that, regular regulatory checks, public attention, and users caring more about privacy all force these firms to take compliance seriously in day-to-day work. Inside the company, leaders also worry about long-term risks and brand image, so many choose to follow rules proactively. What's more, big platforms like app stores now require stricter privacy policies, and these requirements trickle down to small businesses along the industry chain.

In actual operation, SMEs make changes in two ways: process and technology.On the process side, most have redone their user authorization steps. They now ask for clear, separate permission before collecting data, building user profiles, or sending personalized marketing. They also tighten internal data management and make clear who is responsible for data at every stage.On the technology side, they add or update compliance tools: consent management systems, data classification and encryption, and even trial use of privacy-protecting computing to get value from data without breaking the law.

All these changes add up to one big shift: companies are moving away from the old "grow at any cost" model to a more careful, compliance-focused way of running business [3].

3.2 Pathways through Which Compliance Affects Costs, Trust, and Innovation

Compliance affects how small and medium internet firms run their business in three main ways:

First, it hits their operating costs directly. Meeting the PIPL rules means spending money—one-time costs like legal advice, system upgrades, plus ongoing expenses for staff training and regular audits. For SMEs already tight on cash, this pulls money away from marketing and product R&D, putting real pressure on their finances.

Second, it shapes user trust and brand value. When companies handle data openly and follow clear rules, users worry less about privacy and feel more confident. Over time, this trust makes users stay longer, complain less, and recommend the product to others. Privacy protection gradually becomes a hidden, hard-to-copy advantage.

Third, it has a two-way effect on innovation. On one side, strict rules limit some marketing ideas that rely on heavy data mixing or risky algorithm tests, forcing companies to rethink their products. On the other side, regulation pushes them to innovate smarter: they find new ways to market without using sensitive personal data, use anonymous group data for ads, and even turn compliance into a unique selling point.

These three effects work together. Short-term costs do cut into profits, but if firms can turn compliance into real user trust, they'll have a solid base for long-term innovation and growth [4].

3.3 Short-Term Performance Volatility and Long-term Competitive Advantage: Empirical Patterns

Real-world data makes it clear: the Personal Information Protection Law has brought short-term disruptions and long-term splits in how small and medium internet enterprises perform.

In the short term, nearly all companies feel obvious pressure. Customer acquisition gets more expensive because users now go through stricter consent steps. Personalized marketing becomes less accurate, so conversion rates drop temporarily. Direct compliance spending also pushes up administrative costs. All together, these drag down revenue growth and squeeze profit margins.

But as time goes on, companies start to go down very different paths.Firms that only see compliance as a cost and deal with it passively usually keep performing poorly, and some even get pushed out of the market.On the other hand, companies that take compliance seriously and build it into daily work and product design use this shift to organize their data better and manage user relationships more carefully. Even though they also go through short-term fluctuations, they recover faster and gradually earn the benefits of trust—like attracting high-value users who care about privacy, or getting better cooperation and investment opportunities because of their good compliance reputation.

In the long run, the trust and stable operations built from real compliance become new competitive barriers. Small and medium internet firms gradually move away from competing only by traffic and data volume, and build sustainable advantages based on compliance. This trend has already shown clear effects in vertical, user-focused small internet businesses [5].

4. Mechanisms and Dynamic Trade-Offs: In-depth Analysis

4.1 Interactive Model: Compliance Pressure, Resource Constraints, and Adaptive Strategies

To understand why the PIPL affects small and medium internet firms so differently, we can look at how compliance pressure, limited resources, and how companies adapt work together. External regulatory pressure does not directly decide how well a company performs. Instead, it is filtered and shaped by the resources and capabilities the company already has.

Compliance pressure comes from legal rules, how strictly laws are enforced, and potential damage to reputation. It exists on a sliding scale rather than as a simple yes-or-no requirement.

Resource constraints mainly include funding, technical skills, legal know-how, and management time—things most SMEs lack and have in very different amounts.

Companies choose different strategies based on what resources they have:

Companies with more resources take a proactive approach to compliance. They build systems that go beyond the legal minimum and treat compliance as a way to earn user trust and strengthen their brand.

Companies with average resources focus on practical, cost-effective compliance. They meet core legal requirements by optimizing

workflows and using ready-made technical tools.

Companies with few resources only do defensive, minimal compliance. They make the barest changes to get by, which leaves them exposed to legal and operational risks.

These strategies create a self-reinforcing loop. Proactive compliance costs more at first, but reduces long-term regulatory risk and draws users who care about privacy, which in turn improves the company's resource situation. Defensive compliance eases short-term pressure but raises the chance of fines and user loss, making resources even tighter later on.

In the end, a company's performance and competitive edge come from the constant interaction between its strategy and internal and external conditions—not just from legal pressure alone [6].

4.2 Dynamic Equilibrium between Compliance Investment and Economic Returns across Market Contexts

Compliance costs and business returns don't follow a fixed pattern—their balance changes with market environment and time. Key factors include market competition, how much users care about privacy, and the company's own development stage.

In highly competitive markets with similar products, companies care most about quick conversion. If spending heavily on compliance doesn't bring fast results, firms tend to cut compliance budgets, making regulation and growth harder to reconcile.

In niche markets targeting high-value, loyal or privacy-focused users, compliance becomes part of core value and trust. Companies treat it as a necessary investment for entering the market and building brand. The payoff shows up as higher user lifetime value, lower customer acquisition cost, and stronger entry barriers for competitors.

Company maturity also matters. Startups focus on survival and only meet the minimum legal requirements. Growing or mature firms with more resources and longer-term vision treat part of their compliance spending as strategic investment for risk control and competitive differentiation.

To reach a stable balance, companies must keep observing market changes and adjusting their own resources. They need to flexibly control how much they invest in compliance, so they can control legal and reputation risks while maximizing business value under current conditions [7].

4.3 Optimized Pathways and Strategic Recommendations (Case-based)

Based on theoretical analysis, dynamic balance studies, and real cases of small and medium internet enterprises, we have summarized practical strategies for adapting to compliance requirements:

Turn compliance from a cost burden into a value driverInstead of just checking boxes to meet rules, embed privacy protection into product design and user experience. For example, simple and clear privacy settings not only satisfy legal disclosure duties but also give users more control, strengthening trust and making compliance a positive experience for users.

Allocate compliance resources in a targeted and tiered waySort out all data usage scenarios and rank them by risk level. Focus limited resources on core, high-frequency, high-sensitivity business links to control key risks. For non-core or low-risk businesses, use standardized, automated lightweight tools to avoid wasting resources on one-size-fits-all investment [8].

Use privacy-enhancing technologiesApply technologies like federated learning, differential privacy, and secure multi-party computation where appropriate. These tools keep raw data safe while allowing companies to gain useful analysis results, striking a balance between compliance and data value.

Build external cooperation networksRefer to standards and shared templates from industry associations. Work with third-party compliance service providers to reduce the cost of building in-house systems. Cooperate legally with complementary enterprises on data usage to create more value without violating privacy rules.

These strategies help companies move from passive, fragmented rule-following to a systematic, flexible approach that integrates privacy and data compliance into core business stability and innovation capabilities.

5. Conclusion

After China's Personal Information Protection Law came into effect, small and mid-sized internet companies have gradually moved away from the old way of collecting and using data freely. Instead, they're shifting toward a more focused, compliance-driven approach to

marketing. Yes, this transition brings short-term cost pressures and some strategic headaches. But getting compliance right helps build lasting user trust, lowers legal risks, and over time creates real competitive advantages.

What's really going on underneath is a tricky balance between outside regulatory pressure, internal resources, and how flexibly a company can respond. The ones that succeed aren't just checking boxes-they're making smart trade-offs and weaving compliance into how they innovate their business models.

Looking ahead, companies need to get better at protecting privacy while still getting value from data, all within the legal framework. And for policymakers, the next step is to make rules clearer and enforcement more flexible. That way, we can build a digital economy that protects people's rights while still encouraging real, sustainable innovation.

Acknowledgments

This paper is supported by 2025 Research Funding Project of Zhengzhou Sias University (Project Number: 2025XKE116)

References

[1] Hou, T.L. (2026). Research on Innovative Paths of Marketing for Small and Medium-sized Enterprises under the "Internet Plus" Initiative. Modern Business Research, (1), 100–102.

[2] Jiao, Z. (2025). Research on Collaborative Marketing and Credit Strategies for SMEs in Internet Finance. Marketing Circle, (11), 131–133.

[3] Zhang, J.Y. (2025). Optimization of New Media Marketing for SMEs in the "Internet Plus" Era. Sales & Market, (2), 61–63.

[4] Shu, B. (2024). Upgrading and Innovation of Marketing Strategies for SMEs in the Mobile Internet Era. Economist, (7), 280–281.

[5] Yang, Z.L. (2024). Enterprise User Information Compliance Management under the Personal Information Protection Law. Journal of Hebei Open University, 29(3), 55–57.

[6] Xing, Y. (2025). Corporate Compliance Obligations and Proposals under the Personal Information Protection Law. West China Review, (3), 75–78.

[7] Pan Hongjing. Research on Compliance Governance of Corporate Data from the Perspective of Personal Information Protection Law [D]. Harbin University of Commerce, 2024.

[8] Li Yonghong, Dou Wenzhu. Discussion on the Impact of the Personal Information Protection Law on Corporate Compliance and Recommendations [J]. Chinese and Foreign Corporate Culture, 2022, (08):96-98.

