Asia Pacific Science Press

Asia Pacific Economic and Management Review
ISSN(O):3005-9275
ISSN(P):3005-9267
Vol. 2 No.5 (2025)

The Manipulative Mechanisms and Multifaceted Impacts of Dark Patterns in Social Platform: A Case Study of Xiaohongshu

Xiaoyu Huang*

JT Academy, Beijing, 100000, China

Corresponding author: Xiaoyu Huang, 17703320600@163.com

Copyright: 2025 Author(s). This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY-NC 4.0), permitting distribution and reproduction in any medium, provided the original author and source are credited, and explicitly prohibiting its use for commercial purposes.

Abstract: This study explores the phenomenon and impact of Dark Patterns on social platform such as Xiaohongshu. Dark Patterns, like “Bait and Switch”, and “Confirmshaming”, are user interface design choices that benefit the social platform by coercing, steering, or deceiving users into making unintended and potentially harmful decisions. These manipulative practices exert negative impacts on users, publishers, and society at large, such as information cocoon and privacy leak. In order to mitigate these influences and protect users’ rights, this study advocates for legislation and the establishment of digital models to regulate Dark Patterns.

Keywords: Dark Patterns; Social Platforms; Manipulation

Published: Sept 4, 2025

DOI: https://doi.org/10.62177/apemr.v2i5.590

1.Introduction

With the rapid advancement of technology and information proliferation, human attention has emerged as an increasingly scarce resource. The more attention a platform captures, the higher the likelihood that users will visit online stores, prompting social platforms to revolutionize how people socialize and access information. Through sophisticated algorithms and personalized, precise services, many platforms strive to deliver high-quality user experiences.

However, these same algorithms are exploited by profit-driven platforms to collect user data and manipulate behavior, giving rise to Dark Patterns, tactics that induce users to take actions that benefit the platform but align with neither their true intentions nor best interests. Dark Patterns typically exploit cognitive biases to prompt online consumers to purchase unwanted goods or services, or disclose personal information they would rather keep private (Luguri & Strahilevitz, 2021).

Platforms fuel user dependence and addiction by leveraging psychological triggers (e.g., variable rewards) and behavioral biases (e.g., loss aversion), leading many users to unknowingly spend excessive time on these platforms. Meanwhile, high switching costs and loyal user bases make it difficult for users to switch to competing platforms, undermining fair market competition.

Several European and American countries have implemented legislative safeguards in areas like privacy and antitrust, such as the Federal Trade Commission Act and Kids Online Safety Act, to curb these harms. However, these regulatory efforts are limited. They only address the most severe abuses, leaving Dark Patterns underregulated and understudied despite their widespread negative impacts. Nevertheless, the growing academic attention to Dark Patterns highlights the need to analyze

their types, characteristics, and consequences while proposing targeted solutions.

This study examines Dark Patterns primarily through a case study of Xiaohongshu, a leading Chinese social media platform launched in 2013. Alongside giants like Douyin and Weibo, Xiaohongshu has become a staple in Chinese digital life, where users access information through posts and short videos.

As this study will illustrate, Xiaohongshu exemplifies Dark Patterns in action, Convoluted account exit processes. Users face unnecessary hurdles to delete their accounts, discouraging them from leaving. Invasive data collection: The platform aggressively harvests user preference data, for instance, browsing history, likes to refine its algorithms, often without clear consent. Manipulative content ecosystems: Xiaohongshu frequently promotes trending topics and incentivizes creators (via rewards like promotional support) to publish related content, creating a feedback loop that keeps users engaged for longer. These tactics not only erode user trust but also perpetuate a cycle of exploitation, where platforms prioritize profit over user well-being.

2. Definition and Manifestations of Dark Patterns

2.1 Definition of Dark Patterns

Dark patterns, also referred to as "internet traps", were first coined in 2010 by British user interface expert Harry Brignull. The term describes a design approach that uses deceptive interface elements to manipulate users into taking unintended actions. Dark patterns are further defined as "user interface design choices that benefit online services by coercing, steering, or deceiving users into making unintended and potentially harmful decisions" (Mathur A., 2019). They exploit well-documented psychological principles, such as scarcity bias (fear of missing out), social proof (trust in others' choices), and loss aversion (avoiding perceived losses), to drive user behavior. In summary, dark patterns combine tactical interface design with the exploitation of users' psychological traits to boost short-term platform engagement. However, this comes at a cost: they erode user trust and undermine long-term brand or service sustainability.

2.2 Manifestation of Dark Patterns

In the digital era, amid an overwhelming abundance of information, human attention has become a scarce commodity. The more attention a platform can capture, the greater the likelihood of driving user visits and online purchases——making attention the lifeblood of modern digital business models.

This is the core driver behind the rise of Dark Patterns: platforms leverage deliberate design tactics to maximize user engagement time, harvest data for targeted advertising revenue, and outcompete rivals in a crowded market. As competition intensifies, these tactics evolve, with newer, more sophisticated Dark Patterns emerging on platforms like Xiaohongshu. Below are key manifestations of this phenomenon:

1. Disguised Advertising/Native. Manipulation Posts marked "Brand Partner" or "Sponsored" are seamlessly embedded into organic content feeds, mimicking genuine user recommendations to obscure commercial intent at first glance. For example, cosmetics or daily necessity ads are often subtly woven into lengthy, narrative-style posts, blurring the line between authentic reviews and paid promotions.

2. Engagement-Driven Design. Features like "endless scroll" (removing natural stopping points) and strategically positioned "Recommended For You" sections capitalize on the "just one more minute" effect, extending user sessions far beyond their intended length. This tactic exploits cognitive inertia, keeping users hooked on the platform for longer periods.

3. Confirmation Bias. Amplification Algorithms prioritize content aligned with users' past interactions and inferred preferences, creating self-reinforcing "filter bubbles" that limit exposure to diverse perspectives. For individuals with low digital literacy or limited cognitive abilities, these "information cocoons" can foster addiction to specific services, while their range of choices gradually and unconsciously shrinks.

4. Obstructed Opt-Out/Privacy. Controls Privacy settings or notification preferences are deliberately made hard to find or understand, often buried in multiple menus or using confusing jargon. For instance, deactivating a Xiaohongshu account requires a week-long review process, and users may experience "fear of loss" (over losing accumulated followers) to deter them from leaving.

5. Choice Architecture. Manipulation Platforms use visual hierarchy, color contrast, or default settings to nudge users toward

preferred actions. A common example is a large, brightly colored "Continue Browsing" button paired with a small, greyed-out "Exit" option——subtly guiding users to stay on the platform rather than leave.

6. Social Pressure Tactics. Tactics like highlighting "X friends liked this" or "Popular in your area" trigger fear of missing out (FOMO) and exploit herd mentality, particularly among individuals prone to irrational decision-making. This encourages conformity and drives engagement by making users feel left out if they don't participate.

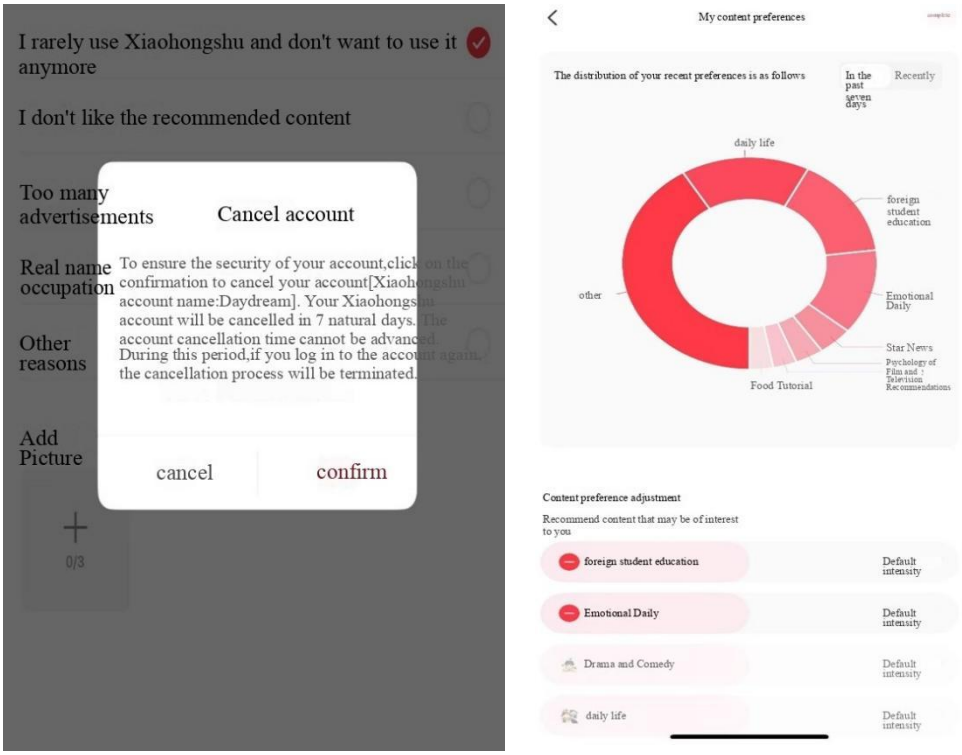
7. Rewarded Sharing. Small incentives (e.g., virtual coins, increased visibility) are offered for sharing app links or inviting contacts——masking extensive data collection in the process. While data itself has no intrinsic value as a production factor, it generates value through dissemination and redistribution, making user sharing a key part of the platform's data ecosystem.

8. Emotional Analytics Manipulation. Sentiment analysis of user-generated content is used to deliver emotionally resonant (and potentially manipulative) content or advertisements. For example, the platform may send push notifications for safety shorts or self-defense sprays to users who exhibit signs of low security awareness, exploiting fear to drive engagement.

9. Drip Pricing. Mandatory fees (e.g., service charges for brand collaborations) are disclosed only at a late stage of a transaction, after users have already invested time or effort in the process. This tactic preys on commitment bias, making users more likely to accept unexpected costs rather than abandon the transaction.

It is worth noting that these Dark Patterns are not isolated. they are systemic, rooted in a business model that prioritizes attention capture and data extraction over user well-being. As platforms compete for scarce user attention, these tactics will continue to evolve, posing growing challenges to digital literacy and consumer autonomy in the years ahead.

Figure 1: Dark patterns on Xiaohongshu



3. The impacts of Dark Patterns

3.1 Impact on Users

The impact of Dark Patterns on platform users is profound, prompting questions about who is most vulnerable to such manipulative practices. Amit (2022) emphasizes that commonly employed Dark Patterns significantly distort user decision-making, with the majority of users displaying similar susceptibility patterns. Age, education level, and income serve as three standard proxies for measuring consumer vulnerability collectively, these factors reflect key traits linked to Dark Pattern susceptibility, including cognitive capacities, impulse buying tendencies, patience, risk-taking behavior, trust, risk tolerance, financial literacy, and digital literacy. Empirical studies highlight a strong correlation between susceptibility and demographic variables: individuals of advanced age, lower educational attainment, or lower income levels exhibit significantly higher

vulnerability, with older adults emerging as a particularly high-risk group. Dark Patterns inflict the most immediate harm on consumers through economic losses. Decisions made under their influence are often involuntary and irrational, as platforms may deliberately push higher-priced products or use interface designs that impede comparative shopping——effectively preventing users from making optimal choices aligned with their best interests. Privacy risks further compound these harms: mandatory login policies (requiring phone numbers or ID cards to access services) can expose personal and sensitive information. This issue is exacerbated by the "multi-platform ecosystem", where social platforms collaborate with other companies to generate revenue——advertising for specific brands while sharing user data with partners. This creates joint information silos that profit at users' expense. With their personal information locked into these ecosystems, users become highly prone to developing addictions to platform services. As Gregory and Abbey note, this addiction stems from dopamine release in the brain, mirroring gambling: random positive stimuli trigger dopamine surges, and repeated exposure fosters dependency, much like compulsive gambling. At its core, the internet operates on an "attention economy". Platforms like Xiaohongshu leverage algorithms and user data to construct "information cocoons" tailored to individual preferences——mechanisms that increase users attention expenditure and personal information costs while diminishing their choices and autonomy. Prolonged engagement with such devices can also trigger physiological issues, including dysregulated cortisol secretion. Even for users aware of Dark Patterns, the constant vigilance needed to avoid them during regular social media use can induce stress and dissatisfaction. Moreover, if users cannot effectively exercise their preferences, both their economic and social efficiency will be significantly diminished.

3.2 impact on platforms and market competition

For private enterprises, the primary operational goal of various platforms is profit maximization, a driving that compels them to adopt such interface designs even though they recognize the unethical nature of Dark Patterns. As a strategic asset that reinforces platform monopolies, data can be converted into strategic investments when entering new markets. Enterprises with substantial data reserves have inherent advantages and potential for horizontal expansion (Li Y. J.). Dark Patterns enable platforms to acquire additional data resources: while this approach may initially boost metrics like Daily Active Users (DAU) and session duration, overreliance on Dark Patterns——instead of improving the quality of information products——will ultimately erode long-term user trust. Platforms associated with manipulative designs risk damaging their reputation and losing users. Moreover, while China's Anti-Monopoly Law has long classified output restrictions as illegal, Dark Patterns undoubtedly constitute a novel form of anti-competitive behavior (Day & Stemler, 2020). First, platforms leverage traffic transmission within their ecosystems to amplify market influence via the multiplier effect, accelerating the expansion of their market dominance. Second, by orchestrating traffic flow dynamics, platforms create a "traffic pool" that directly raises market entry barriers and hinders the growth of potential competitors (Yang & Wang, 2021). If these platforms enter monopoly agreements or abuse their dominant market positions, they will restrict healthy market competition and undermine the fair competition environment. This also disadvantages competitors that adhere to ethical standards and may stifle genuine innovation. Additionally, they may distort the advertising market by artificially inflating engagement metrics.

3.3 Impact on Creators

For content creators, traffic and data revenue are tangible metrics of user engagement. However, driven by the innate psychological need for validation, creators often find themselves manipulated by social media platforms. For example, being coerced into paying to boost post visibility or inserting ads. Under relentless pressure, they are forced to align with algorithmic biases exacerbated by Dark Patterns, often prioritizing sensational or commercially oriented content over authenticity. The distinction between organic and sponsored content has grown increasingly blurred, largely due to the proliferation of native advertising, where shopping links are often embedded in content, eroding creator credibility. Complex visibility algorithms and opaque rules make it harder for creators to reach their audience organically without resorting to paid promotions or manipulative tactics. Furthermore, when creators attempt to leave a platform, they encounter week-long account reviews and warnings of losing all their data and followers.

4. Regulation and Governance of Dark Models on Social Platforms

Addressing Dark Patterns necessitates a multifaceted approach encompassing regulatory measures, platform accountability, and user empowerment.

4.1 Current status of regulation and legislation

From an international perspective, the European Union's Digital Services Act (DSA) explicitly bans specific Dark Patterns, including deceptive nudges and practices that render unsubscribing more cumbersome than subscribing. In the United States, the Federal Trade Commission (FTC) has actively pursued enforcement actions against companies engaging in deceptive practices, most notably in the Amazon Prime subscription cancellation case. Additionally, the Federal Trade Commission Act and Children's Online Privacy Protection Act (COPPA) establish robust legal safeguards for user privacy. China has made substantial progress in regulating Dark Patterns. The State Administration for Market Regulation (SAMR) released the Internet Marketing Guidelines in 2021, which explicitly prohibit practices such as fake likes, misleading comments, and deceptive interfaces. The Cyberspace Administration of China (CAC) focuses on algorithm governance and data protection, while the Personal Information Protection Law (PIPL) grants users enforceable rights over their data, rights often undermined by Dark Patterns. Notably, China's regulatory efforts to protect minors stand out globally, including restrictions on minors' online time and gaming login durations. While enforcement against specific manipulative tactics on major platforms is escalating, comprehensively defining and detecting all Dark Patterns remains a persistent challenge.

4.2 Governance Measures and Recommendations

Dark Patterns manipulate consumer decision-making by deliberately exploiting bounded rationality, limited willpower, and constrained self-interest, constructing sophisticated digital traps in the process. As Yang F. emphasized, "There is an urgent need to conduct in-depth research on establishing appropriate legal frameworks to tackle the misuse of Dark Patterns in e-commerce, thus mitigating the risk of consumer rights infringement at its root." For Government and Regulatory Bodies (e.g., SAMR, CAC) As the primary enforcers of Dark Patterns regulation, government and regulatory bodies like the State Administration for Market Regulation (SAMR) and the Cyberspace Administration of China (CAC) should prioritize the following actions: Firstly, Refine Technical Standards. Formulate and update detailed technical standards mandating that platform interfaces prioritize usability and user control. Existing laws must clearly delineate specific types of prohibited Dark Patterns. Measures such as "online blocking" and "opt-out system establishment" can counter manipulative practices on social platforms. Then, Enhance Enforcement Capabilities. Establish specialized technical teams dedicated to monitoring and investigating Dark Patterns on platforms, strengthening the ability to detect and address violations. Boost Public Awareness. Implement educational and awareness-raising programs while optimizing participation mechanisms to help users understand Dark Patterns and break free from information silos. Foster International Cooperation. Collaborate with global partners to tackle cross-platform manipulative behaviors, as Dark Patterns often transcend national borders. Introduce Behavioral Interventions. Offer platform-switching discounts and subsidies to users and creators to lower the costs of migrating between platforms, reducing reliance on manipulative ecosystems. Finally, Create Incentive Mechanisms. Grant subsidies or tax reductions to platforms that abstain from using Dark Patterns, rewarding ethical design practices.

For Social Media Platforms, as Xiaohongshu, platforms must take proactive steps to eliminate Dark Patterns and prioritize user welfare. Firstly, Establish independent review teams to perform self-assessments and compliance checks, ensuring interface designs align with ethical standards. Secondly, Adopt "Bright Mode" Interfaces. Design interfaces that prioritize clarity, user consent, and ethical control, such as clear advertising labels, one-click opt-out mechanisms, and reasonable privacy settings to empower users. Then, Increase Transparency: Provide consumers and reviewers with detailed explanations of algorithmic principles and content moderation practices, enhancing industry self-regulation and trust. Grant User Control: Give users substantive authority over algorithmic recommendations and data usage, preventing manipulation via "information cocoons" created by platform settings. Finally, Invest in User Education: Offer in-app or on-platform educational resources (e.g., tutorials, awareness campaigns) to elucidate platform operational mechanisms and potential manipulative strategies, helping users make informed decisions.

For Users and Civil Society, empowering users and civil society is critical to combating Dark Patterns. Firstly, Improve Digital Literacy. Implement programs focused on identifying common Dark Patterns and protective strategies. Strengthening

mathematical literacy will reduce susceptibility to framing bias, status quo bias, and information overload.

Secondly, Support Independent Monitoring. Establish civil society-led public interest organizations to operate independent research and monitoring platforms, providing objective oversight of platform practices. Then, Encourage Reporting. Urge users to proactively report privacy violations and manipulative interface designs, creating a feedback loop for accountability. Promote Critical Consumption. Foster thoughtful engagement with online content, raising awareness of persuasive design techniques to help users learn from experience and avoid deception. Lastly, Advocate for User Rights: Push for stronger user rights and platform accountability mechanisms, ensuring platforms are held responsible for manipulative practices.

5.Conclusion

Dark Patterns are a pervasive yet covert form of manipulation deeply embedded in the design of social media platforms like Xiaohongshu. Driven by user engagement metrics and revenue goals, these design tactics exploit psychological biases, erode user autonomy, distort competitive dynamics, pressure content creators, and disproportionately risk vulnerable groups, all in service of boosting interaction and profits.

While regulatory frameworks, especially in China, are gradually evolving to tackle these issues, the dynamic and adaptive nature of Dark Patterns continues to blur their definition and hinder enforcement. Their chameleon-like ability to evade rules complicates both how we classify them and how we police them.

Effective mitigation demands multi-stakeholder collaboration: Regulators must establish clear, actionable guidelines and robust enforcement mechanisms to create a level playing field. Platforms should embrace ethical design principles (e.g., avoiding “infinite scroll” or “confirmshaming”) and boost transparency about how algorithms shape user experiences.

Users need to build digital literacy to recognize manipulative tactics and access tools (like ad blockers or privacy settings) to protect their autonomy. Only through such concerted, cross-sector action can social media platforms fulfill their intrinsic value, connecting people, fostering creativity, and sharing information, without falling prey to the implicit control exerted by manipulative design practices. The future of ethical tech depends on balancing innovation with respect for user agency.

Funding

no

Conflict of Interests

The authors declare that there is no conflict of interest regarding the publication of this paper.

Reference

[1] Luguri, J., & Strahilevitz, L. J. (2021). Shining a light on dark patterns. Journal of Legal Analysis. 2:1-76.

[2] Mathur, A., Acar, G., Friedman, M. J., Lucherini, E., Mayer, J., Chetty, M., & Narayanan, A. (2019). Dark patterns at scale: Findings from a crawl of 11K shopping websites. Proceedings of the ACM on human-computer interaction, 3(CSCW), 1-32.

[3] Zac, A., Huang, Y.C., von Moltke, A., Decker, C., & Ezrachi, A. (2023). Dark patterns and consumer vulnerability. Behavioural Public Policy, 1-50.

[4] Li, Y.J.(2022). The economic implications of data elements and related policy recommendations. Jiangxi Social Sciences, 42(3), 50-63.

[5] Day, G., & Stemler, A. (2020). Are dark patterns anticompetitive?. Ala. L. Rev.,72, 1.

[6] Yang, D. and Wang, R. (2021). On the Impact of Traffic Conduction Behavior on Market Power in Digital Economy Platforms. Financial and Economic Law, (4),11.

[7] State Administration for Market Regulation (SAMR). (2021). Internet Guidelines on Regulating Online Marketing.

[8] European Commission. (2022). Digital Services Act (DSA).

[9] Federal Trade Commission (FTC). (2023). FTC Sues Amazon for Enrolling Consumers in Amazon Prime Without Consent and Sabotaging Their Attempts to Cancel.

[10] Yang, F. (2022). Legal Regulation of Dark Pattern Abuse in E-Commerce. China Circulation Economy,36(8),40-50.