Creativity and Innovation
2025, VOL. 9, NO. 3, 107-111
DOI: 10.47297/wspciWSP2516-252722.20250903

Privacy Policies of Social Platforms under Personalized Recommendation: A China–U.S. Perspective

Shanglin Jiang

Department of Law, Washington University in St. Louis, St. Louis, MO 63130, USA

ABSTRACT
As personalized recommendation becomes a core function of social platforms, concerns over user privacy have intensified. This paper analyzes five representative platforms from China and the U. S. (WeChat, Douyin, Xiaohongshu, Amazon, Meta), and compares their privacy policy structures, regulatory mechanisms, and recommendation practices. Drawing on legal frameworks such as the Personal Information Protection Law (PIPL) and the Federal Trade Commission Act (FTC Act), the study examines differences in data disclosure, user rights protection, and cross-border data flow. It finds that Chinese platforms emphasize detailed data disclosure and local compliance, while U.S. platforms focus on user autonomy and operational convenience. In response to challenges such as "all-or-nothing" consent and secondary/tertiary data usage, the paper proposes improvements in policy design, legal standards, and cross-platform data governance, aiming to strike a balance between user privacy and technological innovation.

KEYWORDS
personalized recommendation; privacy policy; social platforms; China-US comparison; data governance; user rights

1 Problem Statement

As social media platforms become increasingly embedded in daily life, personalized recommendation systems have emerged as a core technology to enhance user experience and extend user engagement. Such systems are commonly defined as tools that analyze user behavior patterns, geographic location, or social connections to customize content and improve interaction efficiency[1]. They are widely applied in advertising, search engines, and social networks. However, while improving service accuracy, these systems have also raised growing concerns about personal privacy. In particular, during the data collection process, platforms often rely on "all-or-nothing" consent models, offer limited options to withdraw consent, and lack transparency regarding data usage—issues that further intensify worries about data misuse and privacy risks. As two major hubs for social media development, China and the United States have adopted distinct approaches in privacy policy design and regulatory frameworks, reflecting different understandings of "user control" and "platform accountability." This paper takes WeChat, Douyin, Xiaohongshu, Amazon, and Meta as representative platforms to compare their privacy policies and legal practices, further exploring the privacy risks associated with personalized recommendation mechanisms and offering suggestions for better governance.

2 Comparative Analysis of Privacy Policies and Legal Regulation on Social Platforms

2.1 Comparison of Privacy Policy Texts

To examine the differences between Chinese and U.S. approaches to data governance on social platforms, this paper compares the privacy policies of five major platforms: WeChat[2], Douyin[3], and Xiaohongshu (China)[4], and Amazon[5] and Meta (U.S.)[6]. The comparison focuses on key aspects such as information disclosure, user rights empowerment, and cross-border data handling.

In terms of how information collection is disclosed, all five platforms involve the processing of user identity data, device identifiers, and behavioral records. However, the presentation logic differs significantly. Chinese platforms tend to list specific permissions and the scenarios in which they are triggered—for example, explaining why and when camera, location, or microphone access is required. Douyin's privacy policy, Article 1.3.1, clearly states: "When you record or publish audio/video or image content, we will request camera, album, and microphone permissions depending on the type of function you use." In contrast, U.S. platforms place greater emphasis on categorizing the purposes of data use. For instance, Meta presents types of data collected in bullet points but rarely details specific use cases. Amazon categorizes data use into eight purposes (such as "improving services" or "providing recommendations"), offering a structured overview but often with general descriptions that lack granular mapping to specific data types and triggers. Compared to Chinese platforms' detailed permission disclosures, the U.S. approach appears less fine-grained.

* **Corresponding Author:** 1062233830@qq.com

Regarding user rights mechanisms, U.S. platforms place greater emphasis on empowering users with active control. Meta and Amazon explicitly enumerate rights such as access, correction, download, deletion, and restriction of personal data processing. More notably, they embed direct links within the policy texts, allowing users to immediately access relevant settings pages. For example, Meta's section "How can you manage or delete your information and exercise your rights?" includes clickable links such as "View and manage your information" and "Port, download or delete your information," significantly lowering the barrier to action. In contrast, while Chinese platforms like WeChat and Douyin also state that users have rights to access, delete, or deactivate their data, they usually guide users with written navigation paths like "[Me - Settings - Account Security]," without direct links. This results in a more cumbersome and less intuitive experience.

As for cross-border data transfer, Chinese platforms generally adhere to the principle of data localization, specifying that personal data is stored domestically and only transferred abroad with legal justification or user consent. They also stress the use of contractual safeguards to ensure data security. U.S. platforms, on the other hand, frequently rely on mechanisms like Standard Contractual Clauses (SCCs) to support international data flows[7]. While these aim to ensure compliance, they are less visible to users, reflecting a commercial logic rooted in globalization.

In summary, while Chinese and U.S. platforms are increasingly aligned in the structural format of their privacy policies, they still differ significantly in data governance philosophies and regulatory priorities. Chinese platforms place greater emphasis on detailed, itemized disclosures and localized compliance safeguards, whereas U.S. platforms focus more on enhancing user autonomy and ease of functional control. Furthermore, in cross-border data transfer mechanisms, China stresses data sovereignty and regulatory boundaries, while the U. S. reflects a stronger logic of global commercial operations. These divergences reveal the two countries' differing understandings of technology governance and user rights, and they lay the groundwork for analyzing the privacy challenges posed by personalized recommendation systems in the following section.

2.2 Comparative Analysis of Legal and Regulatory Practices on Privacy Policies

In the United States, the regulation of privacy policies primarily relies on the Federal Trade Commission Act (FTC Act) and the Fair Credit Reporting Act (FCRA). Section 5 of the FTC Act empowers the Federal Trade Commission (FTC) to prohibit unfair or deceptive business practices[8]. The FTC enforces this by reviewing companies' privacy policies to ensure they do not contain misleading statements or material omissions that may deceive consumers. For example, the FTC brought a complaint against Snapchat, alleging that the platform misled users by claiming that photos sent would disappear after being viewed. In reality, Snapchat failed to inform users that recipients could still save content through third-party apps or screenshots—constituting a deceptive practice in violation of users' privacy rights[9]. In addition, the FCRA imposes strict liabilities—including civil, administrative, and criminal penalties—for unfair or fraudulent conduct in the handling of consumer information[10]. More recently, the U.S. has introduced the American Privacy Rights Act (APRA) of 2024[11], which aims to establish a unified national standard for data privacy, replace the fragmented state-level rules, strengthen protections for sensitive data, and expand individuals' control over their personal information.

In contrast, China's privacy policy regulation is centered on the Personal Information Protection Law (PIPL)[12], which emphasizes strong protection of personal data. Regulatory agencies such as the Ministry of Industry and Information Technology (MIIT) and the Cyberspace Administration of China (CAC) have implemented targeted enforcement actions to ensure the compliance of apps and platforms. For example, the MIIT has continuously carried out special rectification campaigns against apps that infringe upon user rights, issuing public notices and requiring corrective measures[13]. Furthermore, China has established a dedicated App Governance Task Force, jointly guided by the CAC, MIIT, Ministry of Public Security, and the State Administration for Market Regulation[14]. This task force works in collaboration with industry associations to evaluate the privacy policies and data practices of widely used apps, supporting regulatory bodies in achieving effective oversight and compliance enforcement.

In summary, both the U.S. and China have developed relatively mature legal frameworks for regulating privacy policies. However, they differ significantly in their regulatory focus and approach: the U.S. prioritizes post hoc review and liability enforcement, while China emphasizes proactive compliance standards and a systematic administrative oversight model. This divergence in governance philosophy also profoundly shapes how each country responds to the privacy risks associated with personalized recommendation systems.

3 Privacy Challenges in Personalized Recommendation Systems

A comparative review of privacy policy texts and regulatory practices between China and the United States reveals that, although Chinese and U.S. platforms respectively emphasize "compliance obligations" and "user rights," users in both jurisdictions continue to face significant privacy challenges in the context of personalized recommendation. This

section focuses on platform practices to further examine the privacy risks embedded in user consent, data processing, and platform cooperation mechanisms.

3.1 Challenges in the Application of the Notice-and-Consent Principle

With the widespread adoption of personalized recommendation systems, the traditional notice-and-consent principle faces mounting difficulties. This principle requires platforms to clearly inform users of the purpose, scope, and method of data processing before collection and to obtain their voluntary and explicit consent. However, in actual platform operations, this principle is often reduced to a formality—embedded in compliance texts that fail to provide users with substantive protection.

3.1.1 "All-or-Nothing" Consent Models

First, the "all-or-nothing" consent model significantly undermines user autonomy. As noted by some scholars, the notice-and-consent mechanism is frequently misused in privacy policies, functioning more as a form of legal disclaimer than as a meaningful empowerment of user control[15]. On Chinese platforms such as WeChat, Douyin, and Xiaohongshu, personalized recommendation services are typically enabled by default. Users must manually opt out by disabling each associated permission individually, and refusal to authorize data access often results in reduced functionality or restricted access to the service. Faced with a "take-it-or-leave-it" scenario, users are compelled to accept the full terms, resulting in consent that lacks genuine voluntariness.

3.1.2 Lack of Effective Mechanisms for Consent Withdrawal

Second, users' ability to withdraw consent remains inadequately protected. Although Article 15 of the PIPL of China explicitly grants individuals the right to withdraw consent, this right is rarely enforced in practice[16]. Existing legislation does not clearly define the conditions, procedures, or legal consequences of exercising such a right. Moreover, the academic community remains divided on the legal nature of consent withdrawal—whether it constitutes a revocation or rescission of intent—and whether it should follow the general rules applicable to declarations of intent under civil law[17]. This ambiguity further weakens the enforceability of user control in data processing scenarios.

3.2 Data Collection Mechanisms and Privacy Risks

3.2.1 Controversy over the Legitimacy of Data Collection Purposes

According to Article 6 of the PIPL, the collection of personal information must serve a clear and legitimate purpose and be limited to the minimum scope necessary for achieving that purpose. In practice, however, the assessment of whether a data collection purpose is "legitimate" often lacks uniform standards. Judicial determinations frequently rely on individual judges' discretion[18], while academic discourse offers only general principles—such as evaluating the legitimacy in light of specific processing scenarios and behaviors[19] —resulting in fragmented legal application and insufficient constraints on platform data practices.

3.2.2 Secondary Use: Reuse of Processed Data

Even when users initially consent to data collection, platforms frequently engage in what may be termed "secondary use," where collected data is further analyzed and processed to construct user profiles, thereby enhancing the accuracy of personalized recommendations. However, users typically lack effective means to reject or delete such processed data. Some platforms do offer a "disable personalized recommendation" option—for instance, Douyin's Privacy Policy Article 3.1.5(a) states that users who opt out will no longer receive recommendations in the "For You" section but can still browse non-personalized content such as the "Following" feed. Nevertheless, the policy does not clarify how data collected prior to disabling personalization is handled, thereby weakening users' ability to meaningfully control their data.

3.2.3 Tertiary Use: Cross-Platform Data Sharing

A more serious issue lies in the cross-platform flow of user data. In the broader digital ecosystem, personalized recommendation increasingly relies not just on a single platform's internal data processing, but also on collaborative data practices across platforms—known as "cross-platform data sharing" or "tertiary use." In practice, different companies may share user information with each other without obtaining renewed consent from the data subject, aiming

to jointly improve the precision of their recommendation systems[20]. This practice enables user data to circulate across multiple entities, effectively eroding original data boundaries and further diminishing users' control over how and where their personal information is used.

4 Policy Recommendations for Enhancing Privacy Protection on Social Platforms

In light of the gaps identified in previous sections—namely, the structural differences in privacy policy texts, divergence in legal enforcement models, and compliance challenges in the implementation of personalized recommendation systems—this paper offers the following three recommendations to improve transparency in data governance and enhance user control over personal information.

4.1 Improving the Readability and Transparency of Privacy Policies

While Chinese platforms often provide detailed lists of personal data types collected, permission requests, and corresponding usage scenarios, the overall presentation tends to be lengthy and densely structured. This can lead to information overload, making it difficult for average users to grasp key content. By contrast, Meta's privacy policy employs a user-friendly interface with illustrations, short videos, and interactive hyperlinks. For instance, in the section of information managing and deleting, it embeds clickable buttons such as "View and manage your information" and "Port, download or delete your information," significantly lowering the barrier to user understanding and engagement. To shift from "formal compliance" to "genuine informed consent," Chinese platforms are encouraged to adopt modular design structures, highlight key terms, incorporate interactive explanations, and better align the content with actual user scenarios to enhance both clarity and accessibility.

4.2 Strengthening Legal Frameworks and Data Rights Protections

User consent mechanisms remain overly formalistic, particularly regarding the right to withdraw consent. Although the PIPL grants this right, it lacks detailed procedural guidance on technical implementation, platform obligations, and legal effects, resulting in practical difficulties in exercising this right. It is recommended that future legislation provide more specific standards for consent workflows, clarify judicial interpretations of principles such as "data minimization" and "purpose limitation," and establish clear limits on secondary and tertiary uses of data by platforms.

4.3 Enhancing Regulation and Cross-Platform Data Governance

Given the growing risks posed by cross-platform data sharing, regulatory oversight of data flows between platforms should be strengthened. Currently, unauthorized data exchange between third-party platforms may lead to the reconstruction of user profiles and breaches of privacy boundaries. China may draw lessons from the FTC enforcement practices regarding deceptive data use, especially by increasing scrutiny over data transmission paths and collaborative mechanisms behind personalized recommendations. Additionally, efforts should be made to establish clear inter-platform accountability and auditing systems, thereby clarifying responsibilities and improving the overall transparency and coordination of cross-platform data governance.

5 Conclusion

As algorithm-driven personalized recommendation becomes a core function of social platforms, the collection and processing of user data has grown increasingly complex and far-reaching. This paper compares the privacy policies and regulatory frameworks of leading platforms in China and the United States, revealing distinct approaches to data governance and their implications for user privacy protection. Building on this comparative analysis, and in light of the risks posed by personalized recommendation systems, the paper proposes improvements across three key dimensions: enhancing the readability of privacy policies, strengthening user rights protections, and advancing cross-platform data governance. Looking forward, only under a governance framework that is transparent, controllable, and collaborative can a dynamic balance be achieved between technological innovation and individual privacy rights—ultimately enabling the sustainable development of social platforms in a compliant and responsible manner.

References

[1] Toch, E., Wang, Y., & Cranor, L. F. (2012). Personalization and privacy: A survey of privacy risks and remedies in personalization-based systems.

User Modeling and User-Adapted Interaction, 22(1–2), 203–220. https://doi.org/10.1007/s11257-011-9110-z

[2] Tencent. (n.d.). *WeChat Privacy Protection Guidelines*. Retrieved May 14, 2025, from https://weixin.qq.com/cgi-bin/readtemplate?lang=zh_CN&t=weixin_agreement&s=privacy

[3] Douyin. (n. d.). *Privacy Policy*. Retrieved May 14, 2025, from https://lf3-cdn-tos. draftstatic. com/obj/ies-hotsoon-draft/douyin_agreement/380006f8-6557-4965-b545-33a97625d9f5.html

[4] Xiaohongshu. (2025). *Privacy Policy*. Retrieved May 14, 2025, from https://agree.xiaohongshu.com/h5/terms/ZXXY20220509001/-1#a

[5] Amazon. (n. d.). *Amazon Privacy Notice*. Retrieved May 14, 2025, from https://www. amazon. com/gp/help/customer/display. html? nodeId=GX7NJQ4ZB8MHFRNJ#GUID-8966E75F-9B92-4A2B-BFD5-967D57513A40__SECTION_467C686A137847768F44B619694D3F7C

[6] Meta. (n.d.). *Privacy Policy*. Retrieved May 14, 2025, from https://www.facebook.com/privacy/policy/

[7] Meta. (2021, March). *Steps we take to transfer data securely*. Meta Newsroom. https://about. fb. com/news/2021/03/steps-we-take-to-transfer-data-securely/

[8] Federal Trade Commission Act, 15 U.S.C. § 45 (2024).

[9] *In the Matter of Snapchat, Inc.*, Fed. Trade Comm'n, Docket No. C-4501, 2014 WL 1993567 (May 8, 2014).

[10] Li, Yanshun. (2019). Compliance review and improvement of privacy policies of mobile applications in China: A textual study based on 49 privacy policies. *Journal of Law and Commerce Studies*, 36(5), 26–39. https://doi.org/10.16390/j.cnki.issn1672-0393.2019.05.004

[11] Congressional Research Service. (2024). *The American Privacy Rights Act*. Retrieved from https://www.congress.gov/crs-product/LSB11161

[12] Personal Information Protection Law of the People's Republic of China, Article 6. (2021). *Personal Information Protection Law*. Retrieved from https://personalinformationprotectionlaw.com/

[13] Ministry of Industry and Information Technology of the People's Republic of China. (2019, October 31). *Notice on Carrying Out Special Rectification Work for APPs Infringing on Users' Rights and Interests*. Retrieved May 14, 2025, from https://www. gov. cn/zhengce/zhengceku/2019-11/13/content_5451505.htm

[14] Cyberspace Administration of China, Ministry of Industry and Information Technology, Ministry of Public Security, & State Administration for Market Regulation. (2019, January 23). *Announcement on the Special Governance of Illegal Collection and Use of Personal Information by Apps*. Retrieved May 14, 2025, from https://www.gov.cn/zhengce/zhengceku/2019-11/11/content_5450754.htm

[15] Wanfang. (2019). The principle of informed consent and its distortion in privacy policies. *Journal of Legal Science (Northwest University of Political Science and Law),* 37(2), 61–68. https://doi.org/10.16290/j.cnki.1674-5205.2019.02.010

[16] Sun, Z., & Li, R. (2024). From the right of revocation to the right of termination: Cognitive transformation and normative reconstruction of the right to withdraw consent. *Academic Research*, (08), 70–77.

[17] Xiong, B. (2024). Normative positioning and conflict coordination of the right to withdraw personal information consent. *Northern Legal Science*, 19(06), 67–83. https://doi.org/10.13893/j.cnki.bffx.2024.06.002

[18] Lü, S. (2024). A dynamic system theory for assessing the legitimacy of personal information processing purposes. *Legal Science*, (08), 117–131.

[19] Yang, H. (Ed.). (2022). *Interpretation of the Personal Information Protection Law of the People's Republic of China* (p. 28). Law Press.

[20] Guo, C. (2021). The "third-time use" of personal information by personalized recommendation systems: Privacy protection dilemmas in the era of big data. *Science & Technology Communication*, 13(18), 159–161. https://doi.org/10.16607/j.cnki.1674-6708.2021.18.051