*Special Issue: Comparative Approaches to Studying Privacy: Opening Up New Perspectives*

Social Media + Society
October-December 2024: 1–14
© The Author(s) 2024
Article reuse guidelines:
sagepub.com/journals-permissions
DOI: 10.1177/20563051241301265
journals.sagepub.com/home/sms

# A Triple-Layered Comparative Approach to Understanding New Privacy Policy Practices of Digital Platforms and Users in China After Implementation of the PIPL

**Liming Liu[1] and Yiming Chen[2]**

## Abstract

China enacted its first Personal Information Protection Law (PIPL) on 1 November 2021. However, there is a dearth of systematic research examining the implementation of new privacy policies exercised by digital platforms and user engagement with these policies. This study establishes a triple-layered comparative approach to explore the complexities and particularities of privacy policy practices in Chinese digital platforms. The methodology encompasses the analysis of privacy policies from representative platforms—WeChat, Taobao, and Douyin—alongside user experience garnered through a walkthrough method and insights from 28 interviews with platform users. Through critical discourse analysis, the research revealed that state-dominant policy discourses were ingrained in the formulation of platform privacy regulations to legitimize their authority over user data ownership. The users perceived a strong sense of passive protection, characterized by the rigid "agreement" discourse practices that underscore their vulnerability in everyday digital platform usage. The findings shed light on intricate power dynamics at play between platforms, their privacy policies, and users, which leads to polarized reactions from users toward privacy concerns. By examining the articulation of digital privacy policies as instruments of statecraft, we offer a nuanced view of describing non-Western experiences of privacy values and regulatory practices in the digital age.

## Keywords

PIPL, digital platform, comparative privacy research, privacy policies, China

> "I think Chinese people are more open or less sensitive about the privacy issue. If they are able to trade privacy for convenience, for safety, for efficiency, in a lot of cases, they're willing to do that."
>
> Shen (2018, para. 3)

The quotation above is attributed to Yanhong Li, the CEO of Baidu, China's largest search engine. In 2018, he publicly addressed this giant platform's stance on privacy issues and revealed how it shifts responsibility for privacy insensitivity to users by blaming those who prioritize convenience over privacy. Users criticized his words and pointed out the prevalent problems of serious privacy infringement and invasion on the platform. To address growing online privacy concerns within Chinese society, China's Personal Information Protection Law (PIPL) came into effect on 1 November 2021.[1] This legislation established a guiding framework that mandated platforms to formulate privacy policies under state supervision. It represents one of the three prominent global models of privacy governance (Calzada, 2022) alongside the General Data Protection Regulation[2] (GDPR) and California Consumer Privacy Act[3] (CCPA).

The PIPL is a comprehensive legislation that governs the collection, use, management, and protection of users' personal data by digital platforms (Greenleaf, 2021). In contrast to China's Data Security Law (DSL),[4] which emphasizes public interests and national security, the PIPL emphasizes safeguarding users' personal information online by addressing data processing, individual rights, transparency in data management, and data security. Its provisions specifically

[1] Arizona State University, USA
[2] Xi'an Jiaotong-Liverpool University, China

**Corresponding Author:**
Yiming Chen, Academy of Film and Creative Technology, Xi'an Jiaotong-Liverpool University, IA211, South Campus, No. 111, Ren'ai Road, Suzhou Industrial Park, Suzhou 215123, China.
Email: Yiming.Chen@xjtlu.edu.cn

Creative Commons Non Commercial CC BY-NC: This article is distributed under the terms of the Creative Commons Attribution-NonCommercial 4.0 License (https://creativecommons.org/licenses/by-nc/4.0/) which permits non-commercial use, reproduction and distribution of the work without further permission provided the original work is attributed as specified on the SAGE and Open Access pages (https://us.sagepub.com/en-us/nam/open-access-at-sage).

apply to businesses operating in the digital information era (Creemers, 2022), encompassing user rights such as access, copying, rectification, and consent for private data erasure (see Chapter IV). Creemers (2022) posited that combining the PIPL and the DSL established a distinctive framework for data governance in China.

While the PIPL drew inspiration from and referenced the GDPR enacted in 2018 (Xu et al., 2021; You, 2022; J. Zhu, 2022), it established its own legal framework that incorporated government economic reforms aligned with China's political regime to transform it into an instrument of statecraft (Creemers, 2022). The PIPL differs from the GDPR in that it employs a less centralized enforcement approach (Gao & Xu, 2022) and prioritizes national security considerations when handling personal information (Articles 42 and 43). While it exhibits a "family resemblance" to the GDPR due to their shared legal foundations in personal data protection approaches, it diverges ideologically from Western data governance logic (Creemers, 2022, p. 1). Calzada (2022) suggested that the PIPL would revolutionize data processing methods in China and have far-reaching implications for the data localization of global regulations. It becomes crucial to investigate how digital platforms have implemented the PIPL provisions and users' experiences with privacy protection measures in this new era.

Scholars from diverse disciplines have increasingly explored the design, interfaces, and complexities to gain technology-laden insights for platform privacy policies (Ibdah et al., 2021; Liu, Xu et al., 2022). Previous research regarding users' engagement with privacy policies has often explored users' behaviors and strategies for data management (Masur, 2018; Trepte et al., 2015). However, users might use a subjective cost-benefit analysis guided by privacy calculus to balance their desire for privacy protection, potential risks and benefits, and information disclosure (Culnan & Armstrong, 1999). A comparative approach to privacy research could shed light on situations where these (in)balances affect behavior differently (Capurro, 2005; Esser & Hanitzsch, 2013). While the global impact of China's privacy policies is significant (Kai & Zhou, 2022), further investigation is needed to understand the non-Western-centric privacy values embedded in digital platform practices during the PIPL era.

Previous research on digital privacy in China has primarily focused on users' perceptions of privacy on social media (Chen & Cheung, 2018; Yang & Liu, 2014) and users' trust in the platform's privacy protection (Z. Wang & Yu, 2015). It also compared the distinctions and operational logics of Chinese digital platforms' privacy policies across multinational contexts (Liu, Xu, et al., 2022). Since the implementation of PIPL, scholars have explored its extensive application across Chinese society. You (2022) proposed that the PIPL establish a new power dynamic in privacy protection by shaping collaborations between platforms and the state (Jiang & Zheng, 2023). These timely studies highlighted the necessity of evaluating the PIPL from both platforms and user perspectives. This inspired us to undertake one of the first attempts at adopting a comparative approach to systemically examine how privacy policies have been exercised by platforms and users since the enactment of the PIPL.

This study expands the conceptual framework of comparative privacy research (Masur et al., 2021) to empirically examine digital platforms and practical privacy literacy (Masur, 2020) based on experiences in China. We argue that the authoritarian privacy practice model, as implemented in China, is a dynamic process driven by national interests involving tangled interactions between the state, platform enterprises, and individuals that take place within broader political, cultural, economic, and technical domains. Our comparative approach aims to enhance the understanding of the complexities and uncertainties of the privacy policy landscape in China, despite its resemblance to personal data protection measures commonly observed in the West (Creemers, 2022). For instance, platform enterprises must comply with Chinese national regulations while pursuing commercial interests (Su & Flew, 2021). Given this complexity, this study raises three fundamental research questions (RQs) to compare the interplay between privacy policies and platform users under the PIPL:

> RQ1: How do Chinese digital platforms discursively construct, characterize, and implement privacy policies to comply with the PIPL?
>
> RQ2: How do users make sense of, feel about, and engage with these new policies on Chinese digital platforms?
>
> RQ3: From a comparative perspective, what are the complexities, discrepancies, and commonalities among the platforms and users regarding different platforms' implementation of their privacy policies?

## Literature Review

### The Comparative Privacy Research Framework

Privacy research comprises a multifaceted and ongoing exploration of personal information security that is crucial for understanding the intricate dynamics between individuals, organizations, and governments in contemporary societies. It is also multidisciplinary, encompassing privacy technologies (Avancha et al., 2012; Diaz & Gürses, 2012), privacy laws (Citron, 2019; Richards & Solove, 2010), and various social science perspectives in which privacy is embedded in social, cultural, and political contexts through media and communication studies (Marwick & Boyd, 2014; Masur, 2018). Li (2020) identified societal and institutional privacy concerns among Chinese users and their impacts on government surveillance practices and platform cultures. Liu et al. (2021) investigated how facial recognition payment policies affect individuals' privacy risk management.

Kang and Oh (2023) further examined how smart speaker users can utilize self-efficacy in privacy management to mitigate potential risks while enhancing benefits.

The comparative understanding of privacy concerns has also gained considerable attention for its contribution to intercultural privacy research (Capurro, 2005) and expanded its research boundaries by exploring universally applicable practical studies (Esser & Hanitzsch, 2013). At the platform level, Pekárek and Pötzsch (2009) emphasized the need for a combination of technical, legal, and normative measures to address privacy issues in various digital spaces. At the user level, Liu et al. (2024) compared the discrepancies between privacy concerns and boundary linkage in chatbot usage among users in China and the United States. Similarly, Trepte and Masur (2016) examined cross-cultural differences in privacy protection behaviors through a user-centric lens.

The comparative privacy research framework provides a holistic perspective on the intricate nature of safeguarding privacy and delineates a systematic and multilayered structure for in-depth scrutiny of privacy issues (Masur et al., 2021). This framework facilitates multidimensional comparisons by identifying the interrelated cultural, social, political, economic, and technological structural components for analyzing privacy protection (Masur et al., 2021). Indeed, these components are not mutually independent but can guide us in integrating them together to gain a comprehensive understanding of the intricate interplay of privacy practices among the state, platforms, and users through systematic comparisons at the micro-, meso- and macro-levels (Masur et al., 2021). Significantly, the framework promotes the advancement of research into non-Western approaches to privacy (Dal, 2024). We employ this multi-dimensional-comparative lens to analyze and compare privacy protection practices in China's PIPL regulations, platform policies, and user perspectives, unraveling the various aspects of privacy concerns in China.

## Privacy Practices on Digital Platforms

The academic research on protecting privacy practices of digital platforms is extensive. In the scope of this study, two distinct research veins were identified. The first vein focused on analyzing the mechanisms and impacts of privacy policies from a platform perspective, specifically through the disclosure of their policies to the public in general and daily users. Platforms act as regulators by establishing institutionalized rules through user interactions and usage habits (Crémer et al., 2019). They use their terms of service to establish technical and contractual standards derived from specific privacy and data protection laws (Huckvale et al., 2019). Technology giants such as Apple and Google have incorporated various international privacy and data regulations into their platform policies to ensure user compliance with their products in different regulatory environments (Van Hoboken & Fathaigh, 2021), thereby effectively creating a legal agreement between the users and the platforms. Furthermore, studies in computer and information sciences examined the comprehensibility, readability, and interface design of privacy policies across platforms (Antón et al., 2004; Bonneau & Preibusch, 2010; Proctor et al., 2008). Greene and Shilton (2018) investigated the power imbalances inherent in the design of privacy rules and developers' comprehension of privacy by analyzing platforms' policy guidance.

The second research vein emphasized a literacy lens to understand how individuals exercise privacy protection on different platforms. Privacy literacy has been considered a crucial component of safeguarding individual privacy (Choi et al., 2018; Rössler, 2005), particularly in their daily use of platforms (Park & Jang, 2014; Trepte et al., 2015). Privacy literacy involves articulating interconnectedness with media usage across diverse media contexts. Thus, privacy literacy is frequently conceptualized as an extension of media literacy, recognizing the role of privacy as an essential ingredient of media literacy discourse (De Leyn et al., 2022). In this vein, Pangrazio and Selwyn (2019) developed a comprehensive framework that considered both the social and technical factors involved in personal data generation and processing to understand data privacy. Masur (2020) further conceptualized online privacy literacy as a paradoxical aspect of user self-protection and self-determination by viewing it as a facet of digital media literacies and essential to autonomy and democracy.

## Chinese Digital Privacy Regulations and the PIPL

The extensive use of technology has led to the collection of user data by platforms, thereby making privacy protection a global priority. Two revolutionary initiatives—the GDPR in the European Union and the CCPA in America— have established regional models for privacy legislation (Calzada, 2022). In contrast, the Chinese approach to policymaking in personal privacy differs from Western regulatory and protective measures in that it encompasses a distinct focus on safeguarding the privacy of individual consumers (Moreira, 2023). This outcome resulted from China's significant economic reforms and the adoption of a market economy under its socialist system in the 1980s when privacy became a widespread concept (Cao, 2005). This consumer-centric approach has been reinforced in recent years by the flourishing of Chinese digital platforms, such as Baidu, Alibaba, and Tencent (Jia et al., 2018). With the intense digital privacy problems, the Chinese government has issued several laws and regulations pertaining to (online) personal data protection, such as the Consumer Protection Law (1994) and the Cybersecurity Law (2017), and the Civil Code of the People's Republic of China (Calzada, 2022; Liu, Huang, et al., 2022; H. Wang, 2011).

Grounded in the Constitution of China, the PIPL is an indispensable component of China's cybersecurity laws and its extensive legislation governing personal information protection

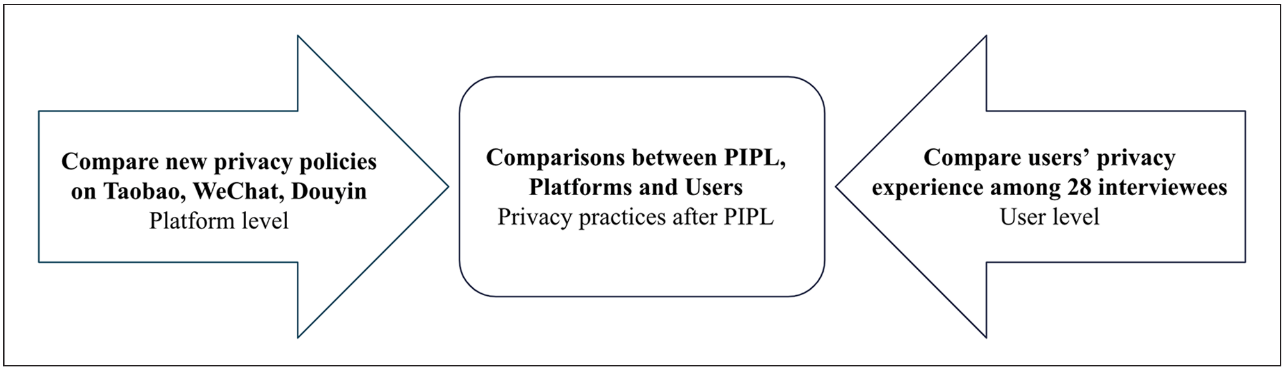

Compare new privacy policies on Taobao, WeChat, Douyin
Platform level
Comparisons between PIPL, Platforms and Users
Privacy practices after PIPL
Compare users' privacy experience among 28 interviewees
User level

**Figure 1.** The triple-layered comparative research design.

(Greenleaf, 2021). The PIPL emphasizes the principle of data localization, imposing restrictions on cross-border transfers of "important data," which potentially leads to an increased concentration of data storage and processing activities within China (Articles 36 and 40). The Chinese government has granted broad authority to relevant authorities under the PIPL for accessing personal data for oversight purposes related to national security, public health, or crime prevention (Article 13). The PIPL also reflects a collectivist approach to privacy that balances individual rights with public interests and national security concerns (Tan & Zhang, 2021). In terms of rhetorical discourse, the PIPL exhibits textual similarities with the GDPR regarding its legitimization of personal information protection and delineation of the significance of data privacy. Both legislations employ terminology such as "personal information processor," which corresponds to the concepts of "data processors" and "data controllers" in the GDPR (See PIPL Article 53; You, 2022). However, unlike the GDPR and the CCPA, the PIPL primarily regulates the relationship between digital technology companies and consumers to prevent cybercrime rather than imposing substantial regulations on governmental entities' collection and utilization of private data (Creemers, 2022). Notably, the definition of "sensitive" data in the PIPL is broader than those of the GDPR or CCPA regulations (Article 28). Administrative penalties with substantial fines can be imposed for non-compliance with the PIPL, but criminal penalties are excluded (Article 66).

Douglas (2000) argued that China's perspective on individual rights differs from the West by primarily attributing these rights to the party, state, and collective entities, thereby implying a power dynamic between individuals and the state aimed at promoting socialist ideals. Consequently, the PIPL aligns with China's centralized governing system (Feng, 2019) and its mechanism for granting individual rights (Douglas, 2000), thus reinforcing the authority of the socialist system and granting substantial control over data governance to the Chinese authorities.

The enforcement of the PIPL has spurred research into how platforms have responded to it. You (2022) viewed the PIPL as a catalyst for reshaping power dynamics between the state, the market, and netizens. For example, Jiang and Zheng (2023) evaluated how health code apps comply with the PIPL to standardize monitoring and control functions over personal health information. However, evidence is lacking in terms of the existing legal-oriented and platform- and user-focused research to demonstrate the law's impact on altering digital privacy in China. Therefore, whether new privacy-related tensions have arisen between platforms and users after the implementation of PIPL remains underexplored.

## Methodology

By immersing ourselves in observing the updates to the privacy regulations of Chinese digital platforms since December 2021, we have come to perceive the formulation of platforms' privacy policies as a multifaceted privacy practice rather than merely textual alterations in policy. Hence, our focus is on examining the practical mechanisms implemented by mainstream platforms and engaging users in discussions to evaluate their comprehension of PIPL-driven platform privacy policies and thus reflect their level of privacy literacy.

To accomplish these aims, we designed a three-layered comparative research approach (see Figure 1) encompassing the platform, user, and PIPL-platform-user levels to investigate the interplay between the tensions inherent in privacy regulations and establish multidimensional comparisons. This approach drew inspiration from Y. Zhu's (2022) study on social media dynamics and state surveillance, which integrated the analysis of governmental authorities, business entities, and consumers to comprehensively understand information networks in China.

Our methodology addressed a research gap by employing a comprehensive comparative framework that examined the top-down and bottom-up approaches to rule-making while analyzing the similarities and differences in their implementation across various platforms in response to the PIPL. Subsequently, it explored the complexities and interactions of privacy practices articulated through governmental regulations, platform policies, and user behaviors. This approach situated our comparative research on privacy practices within a broad spectrum of social factors encompassing politics, culture, and the economy (Masur et al., 2021).

Our research utilized a three-layered comparative design involving three consecutive stages of data collection to comprehensively examine the extensive usage of digital applications in the consumption, socializing, and entertainment domains. We selected Taobao,[5] WeChat,[6] and Douyin[7] as exemplary platforms and gathered texts from the new privacy policies[8] issued by Alibaba, Tencent, and ByteDance, the three Chinese digital giants. Each platform presented a privacy policy statement in a pop-up window on their login or settings pages. By February 2022, after the enactment of the PIPL and subsequent policy updates by the platforms in response to it, we collected these three privacy policy statements as our data corpus.

In the second data collection stage, we specifically employed a parallel walkthrough method (Light et al., 2018) to understand privacy policy practices by leveraging our self-sensing experiences on platforms. This method—a user-centered research approach that involves systematic observations to discern an app's vision, operational model, and governance modes (Ferris & Duguay, 2020; Light et al., 2018)—enhances researchers' understanding of user experiences in digital spaces (Duguay et al., 2024). By executing three sequential steps—registration and entry, everyday usage and app suspension, and closure and leaving (Light et al., 2018)—we actively observed the updating process of privacy regulations as implemented by the three platforms. This included examining the platforms' methods of notifying users about regulatory changes, the design of notification interfaces, and the browsing experiences from the PIPL's implementation in December 2021 until the completion of policy updates on these platforms in June 2022.

During the third stage of data collection, we conducted 28 in-depth interviews with users to gather data on their everyday privacy practices across the three platforms. To obtain the most direct information about the users' experiences regarding the changes in the platforms' privacy policies before and after the PIPL was implemented, we established four specific criteria for participant recruitment: (1) individuals of different genders and professional backgrounds aged at least 18 years old, (2) daily active users of these platforms, (3) users who had used these platforms for at least 5 years, and (4) users who had experienced changes in the platforms' privacy policies. Each face-to-face interview lasted from 45 to 90 minutes and was implemented between June and November 2022.

The study employed critical discourse analysis (CDA) at the analytical level of privacy comparisons to demystify the embedded ideologies and power dynamics through an exploration of discourse, thereby exposing the inherent inequalities between platforms and individual users within a Chinese context (Wodak & Meyer, 2009). Based on our observations, we viewed the privacy policies as formalistic discourse practices that re-structured platform usage in such a way that the users' subjectivity was re-articulated in a discursive framework of direct and obligatory "agreement." As user consent to a platform's privacy policy is a prerequisite for accessing platform services, the users' privacy practices and perceptions have been disregarded. We utilized the principles of CDA to detect sometimes hidden meanings in digital privacy practices by analyzing privacy policy documents and walkthrough experiences, along with user interviews (Fairclough & Wodak, 1997).

## Platform Level: Comparing the Practices of New Privacy Policies on Taobao, WeChat, and Douyin

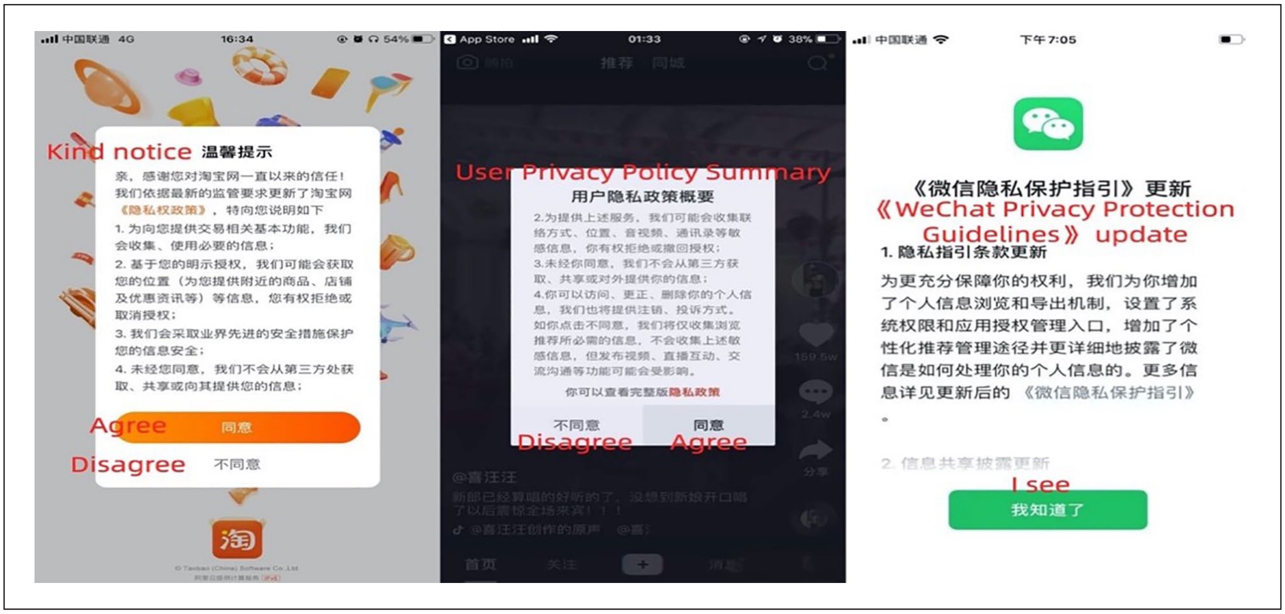
### *Uniformity of the Notification Models of the Privacy Policies*

This section illustrates that subsequent to the enactment of the PIPL, the three platforms opted for direct and timely communication with their users by delivering forceful notifications and clearly delineating their privacy policies' boundaries, thereby elucidating the shared relationship, status, and interests between the users and the platforms.

The PIPL clarified the necessity of digital platforms practicing transparency to ensure "truthful, accurate, and comprehensive information disclosure" in "an easy-to-notice manner" and "in clear and easy-to-understand language" when collecting users' personal data (Article 17). Through our walkthrough method, we found that each platform (see Figure 2) was obligated to promptly update its privacy policy and notify users accordingly. All three platforms implemented a push notification system as their approach and required user consent to continue utilizing the platforms. This mandatory agreement-oriented notification model ensured optimal user service and aligned with the PIPL's legal framework.

Moreover, the three platforms reinforced their notification methods to communicate their privacy policy updates to users in a straightforward and effective manner. WeChat claimed that significant changes in their policy terms generated push notifications, pop-up reminders, or other legally compliant forms of notification. Douyin stressed the importance of obtaining users' re-consent to the updated policies and primarily notified users through instant messages to ensure their awareness. Similarly, Taobao highlighted the significance of users' agreement with its policy updates and provided a dedicated page that explained the changes made to their privacy policies.

The notification mode further strengthened the correlation between the platform's privacy policy and other associated policies, such as those that governed ByteDance's additional products and those implemented by its parent company, thereby constituting an integral aspect of Douyin's comprehensive approach to safeguarding user privacy. Douyin unequivocally underscored its unwavering commitment to prioritizing user



Kind notice 温馨提示

亲，感谢您对淘宝网一直以来的信任！我们依据最新的监管要求更新了淘宝网《隐私权政策》，特向您说明如下

1. 为向您提供交易相关基本功能，我们会收集、使用必要的信息；

2. 基于您的明示授权，我们可能会获取您的位置（为您提供附近的商品、店铺及优惠资讯等）等信息，您有权拒绝或取消授权；

3. 我们会采取业界先进的安全措施保护您的信息安全；

4. 未经您同意，我们不会从第三方处获取、共享或向其提供您的信息；

Agree 同意

Disagree 不同意

User Privacy Policy Summary

用户隐私政策概要

2.为提供上述服务，我们可能会收集联络方式、位置、音视频、通讯录等敏感信息，你有权拒绝或撤回授权；

3.未经你同意，我们不会从第三方获取、共享或对外提供你的信息；

4.你可以访问、更正、删除你的个人信息，我们也将提供注销、投诉方式。

如你点击不同意，我们将仅收集浏览推荐所必需的信息，不会收集上述敏感信息，但发布视频、直播互动、交流沟通等功能可能会受影响。

你可以查看完整版隐私政策

不同意 Disagree

同意 Agree

《微信隐私保护指引》更新

《WeChat Privacy Protection Guidelines》update

1. 隐私指引条款更新

为更充分保障你的权利，我们为你增加了个人信息浏览和导出机制，设置了系统权限和应用授权管理入口，增加了个性化推荐管理途径并更详细地披露了微信是如何处理你的个人信息的。更多信息详见更新后的《微信隐私保护指引》。

2. 信息共享披露更新

I see

我知道了

**Figure 2.** The notifications used by (from left to right) Taobao, Douyin, and WeChat.

data protection within ByteDance's overarching framework. This policy endeavored to offer exhaustive directives for users pertaining to personal information gathering and management across the different iterations and features of Douyin. On the contrary, WeChat maintained differences between domestic and international contexts when formulating its guidelines concerning user data protection and delineated the legal boundaries of its China-centric privacy policy.

## *Differences in the Rights Granted to Users*

This section demonstrates how different platforms have granted user rights in accordance with PIPL. The three platforms faced the challenge of striking a balance between the direct and the discretionary rights bestowed upon users. They shared a similar understanding of granting direct rights to users in terms of the PIPL framework, which mandated that individuals should "be informed," "make decisions on the processing of their personal information," "restrict or refuse the processing of their personal information by others," and "consult and duplicate their personal information from personal information processors" (Articles 44 and 45). However, differences in the discretionary rights offered by each platform reflected their respective interpretations of their legal obligations under the PIPL.

In terms of deletion, browsing, review, and cancelation exercises on these platforms, users were entitled to exercise their rights to access and modify their account information, chat history, device information, and other personal data. However, Taobao's policy provided more specific regulations regarding these direct rights by mandating the assistance of the customer service department to safeguard users' legitimate rights concerning information processing on the platform.

Aside from the mandatory rights stipulated by the PIPL, the three platforms implemented distinct discretionary rights for users. To safeguard user privacy on Taobao, WeChat, and Douyin, users were provided with the option to customize their interests to minimize algorithmic recommendations for content and advertisements. By reducing reliance on algorithms, it has become more challenging to accurately predict user behavior patterns, which enhances information security. Users were only allowed to modify or disable personalized advertisements, while programmed advertisements remained unchanged in terms of quantity. Consequently, these optional rights led to limited collection and usage of platform users' personal information. WeChat explicitly stated in its policy that users can cease using the "contacts" feature, thereby suspending the recommendation of their contact details to individuals who have already acquired them.

Differences were also detected in terms of the diverse translations of the PIPL by the three platforms. For instance, while Taobao's policy situated its right of information disclosure within the framework of national law violations, it further expanded this right by asserting that Taobao could disclose information in cases where users severely breach the Taobao agreements and regulations. Conversely, WeChat adopted a compassionate policy that allowed bereaved relatives to request information about deceased users, which aligned with Article 49 of the PIPL's provisions on sharing information about deceased individuals.

### Utilizing and Protecting Users' Information on the Platforms

This section analyzes the user rights conferred by these platforms, with a specific focus on their utilization and protection of user information. The obligations of personal information processors are outlined in Chapter V of the PIPL; however, a precise definition is not provided. These platforms strategically solidified their comparable legitimacy through alignment with regulatory and legal discourses to justify their approaches toward collecting, utilizing, and safeguarding user information. They accomplished this by asserting ownership of users' data and implementing advanced technologies for privacy protection. Nevertheless, each platform adopted a different discursive focus: Taobao employed a retrospective strategy centered around usage history analysis; WeChat utilized a localization strategy for data processing to ensure encryption and prevention at the local device level; Douyin implemented an authorization strategy to reassure users by obtaining certifications for protective technology.

Taobao and Douyin have divergent approaches to information ownership in their policies. Taobao stressed its retroactive declaration by highlighting that its utilization of user data is predicated on individual users' historical usage patterns. That is, it determined the permissibility of its employment of users' private information by analyzing their browsing history, shopping activities, and service records. WeChat established robust privacy protection measures that encompassed local encryption of confidential data on users' devices; prevention of viruses and the installation of Trojans horses and malicious software; and identification of fraudulent activities, account thefts, impersonations, and other illegal acts via its scrutiny of unique device identifiers, login IP addresses, operation logs, and location data.

In accordance with the PIPL's requirements regarding "adopting corresponding security technical measures such as encryption and de-identification" (Article 51), Douyin's policy explicitly claimed that they had adopted software development kit technology to compile and synchronize user accounts and content across different versions of the Douyin application. This approach demonstrated that Douyin employed an authoritative discourse strategy in the policy to promote information protection capabilities through advanced technology. The policy further proclaimed its successful attainment of evaluations for "national information security level protection" and "international authoritative certifications" regarding privacy and security management.

## User Level: Comparing the Privacy Practices of the Three Platforms

### The Platforms' Privacy Practices Perceived as Controversial

This section presents an in-depth analysis of the users' perceptions regarding the privacy practices implemented by the three platforms under study. In the interviews, users reported that Douyin and Taobao engaged in privacy-violating surveillance, which led to the users developing a sense of having been intruded upon by breaches of their personal information. However, despite expressing concerns about data ownership, users consistently voiced their trust in these platforms.

The users pointed out that their in-app activities were subject to surveillance, which compromised their privacy.

> When you say something to others or search for something, for example, Douyin will constantly recommend you more relevant content within seconds or in the following days. This function is a bit too powerful! It makes me feel like I am being monitored all the time, and it seems to capture every word I say. (Interviewee 6)

This phenomenon was closely linked to the algorithmic recommendation systems employed by the platforms. That is, the platforms consistently utilized data tracking to automatically generate personalized content recommendations based on the users' browsing history (Matamoros-Fernández, 2017). Interviewee 4 further stated, "If I'm watching a food video on Douyin, the next ten videos recommended to me are all about food. But sometimes, I don't always like watching the same content but want to switch it up." Such algorithm-driven surveillance can lead to content containment through filter bubbles (Haim et al., 2018) and information cocoons (Gossart, 2014). Nevertheless, surveillance of users' information also occurs across multiple digital platforms, which causes user confusion and apprehension toward surveillance itself, as illustrated by Interviewee 20's unsettling encounter with Douyin and Taobao.

> I was just scrolling through a Douyiner's profile that I don't even follow . . . just browsing some of the beauty and skin care products she recommended in her videos. But then, when I opened up Taobao, those same exact products were popping up on my homepage! I never searched for them on Taobao or anything. It's like these two platforms are spying on me and sharing my data with each other.

The intricate surveillance mechanisms implemented on these platforms pose challenges in comprehending who owns users' information behind the scenes. Certain users raised concerns regarding data and information ownership on these platforms and specifically questioned who owned the user data and information. The example above shows that the ownership issue is intertwined with users' fundamental apprehensions about the privacy of their data and the legitimacy of these platforms' collection, storage, and sharing of private information. Interviewee 24 posed three questions concerning the ownership of the personal data and information that users disclose on these platforms.

> When my data is up for grabs to be traded by these platforms, I want to ask who the owner of the data asset is. Me or the platform? That's the first issue that nobody seems to have a clear

> answer for. Secondly, why can you trade my data without my permission if I haven't traded with you (I mean the platform)? And if you do make money off of it, shouldn't I get a cut too? Then, the last question: why should my information belong to the platform in the first place?

These questions challenged the default assumption that platforms inherently consider users' data and information integral to company assets. In fact, collecting user data and information has become an intrinsically essential process in maintaining a platform's dominance (Fenton et al., 2020). However, the practical effectiveness of privacy policies regarding data ownership remained ambiguous and confusing, thereby undermining users' trust in the platforms.

In addition to concerns regarding user surveillance and data ownership, the users also showed varying levels of trust in the privacy practices of these platforms. The users employed diverse criteria for assessing platform trustworthiness, including factors such as a platform's overall reputation, user base size, and societal impact. The users maintained trust in these platforms, as evidenced by Interviewee 10's statement that "China has over a billion people using these platforms" and Interviewee 21's assertion that "information security incidents are unlikely to occur often because they are run by giant companies." WeChat has become the most trusted platform among the three platforms considered here because it "intertwines both life and work." Users trust it because "it does little harm even if it violates my privacy" (Interviewee 23). However, the users questioned Douyin's and Taobao's potential violations of user privacy through their recommendation systems. When considering Taobao's online shopping recommendations, Interviewee 20 argued that Douyin was the least private among the three platforms because it recommended connections with "people you may know and show you the content your friends liked," "users in the same city and area," and "contacts based solely on your mobile number."

### *Constrained Rights Versus Invisible Self-Management*

This section explores the constraints on users' privacy rights and their lack of effective platform self-management. On one hand, the users perceived a curtailment of their autonomous right to privacy due to the absence of alternative options for information management. Furthermore, when a user's private information was exposed, the platforms failed to provide mechanisms for lodging complaints. Conversely, the users demonstrated varied yet inconspicuous forms of self-management regarding their personal data.

According to Article 17, platforms must notify users about their privacy policies (PIPL, 2021). However, the users perceived a lack of personal agency on these platforms and felt compelled to comply with their policies. Interviewee 8 explained that the platforms utilize two primary methods to inform users about their privacy policies: direct pop-up notifications and mandatory read-click notifications.

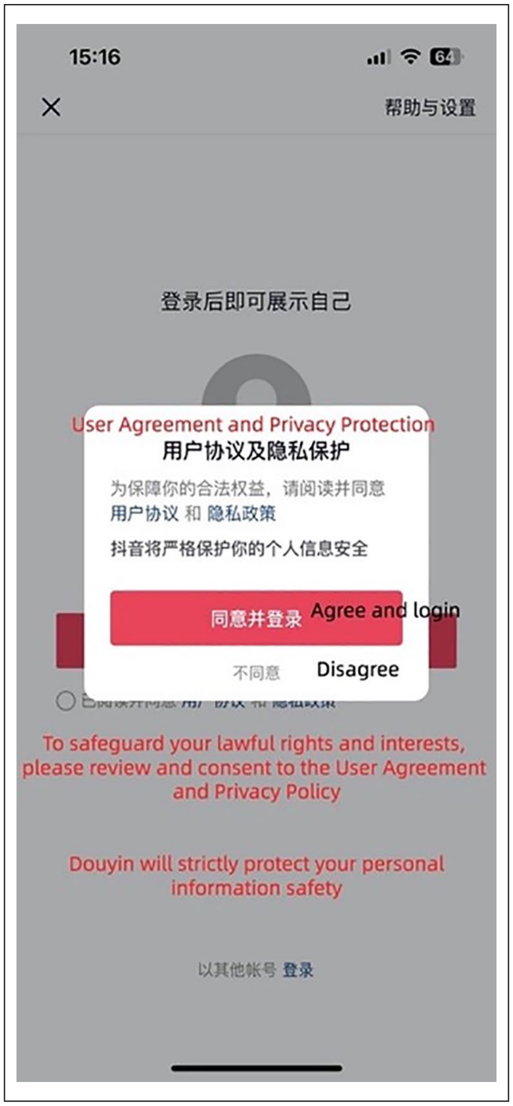
> So, when you open the app, either a little box will pop up for you to tick "agree" before logging in, or the whole privacy policy will appear. But if it's the latter, don't worry—the page will freeze for five seconds so you can read it properly and then click to agree before moving on.

Interviewee 17 described her consistent practice of providing consent to the privacy policy on Douyin each time she accessed her account. As depicted in Figure 3, from the walkthrough, a notification regarding privacy protection and terms of service appeared before logging in. Therefore, consenting to the privacy policy became an obligatory prerequisite for continued usage of the applications, as summarized by Interviewee 23: "Without agreeing, I cannot use this app."

Concerns were also raised by the users regarding the potential exposure of their private information on e-commerce platforms, particularly Taobao, during product purchases. The inherent nature of online shopping makes it easy for others to access users' personal addresses and contact details. Interviewee 3 highlighted the inadequacy of the complaint mechanisms in cases when private information was compromised on Taobao. Her phone number and address were disclosed after she purchased on Taobao, which resulted in persistent harassment from the online merchant following her negative product review. She received incessant calls and messages urging her to revise the review. Subsequently, she "gathered all the evidence and reported this to Taobao officials" but "never heard back from them" (Interviewee 3).

The absence of a functional complaint mechanism renders users in a vulnerable position on these platforms, where their consumption records and personal contacts are easily accessible. Nevertheless, the users still maintained their expectations of attaining enhanced platform privacy rights. As Interviewee 7 indicated, platforms should take effectual actions to protect users' privacy as the "platforms collect all of my data, so they must take robust protective measures to ensure that my data remains secure and confidential." The users believed that the privacy practices of the three platforms aimed to "protect platforms from harmful situations and allow them to avoid potential disputes" (Interviewee 22), while they perceive platform rights as a means for legitimizing their ability to "casually steal and appropriate users' information upon agreement" (Interviewee 9).

The users attempted to exercise covert methods to realize self-management and address these constrained rights, albeit with widely divergent strategies for information management. Interviewee 22 strategically maximized the exposure of her content-related information on Douyin and perceived it as advantageous and conducive to enhancing the platform's convenience. She especially favored allowing the algorithmic system on Douyin to analyze her content preferences because, according to her assertion,



登录后即可展示自己

User Agreement and Privacy Protection

用户协议及隐私保护

为保障你的合法权益，请阅读并同意
用户协议 和 隐私政策

抖音将严格保护你的个人信息安全

○ 已阅读并同意 用户协议 和 隐私政策

To safeguard your lawful rights and interests, please review and consent to the User Agreement and Privacy Policy

Douyin will strictly protect your personal information safety

**Figure 3.** The Douyin privacy policy notification page.

"The platform can recommend to me the content I really want to see when I share my data."

While some users actively disclosed their private information on the platforms, others employed various self-protection strategies to render themselves undetectable. Nevertheless, the users stressed that this protective strategy lacked universality because "all the functions are turned on by default, such as geographical location, tracking, and ad reception, instead of allowing you to choose" (Interviewee 1).

Interviewee 12 emphasized that she "only allow[s] Douyin access to my photos and videos when I use it" to ensure that her visual data remained uncollected by the platform unless she permitted it. Interviewee 8 also used a similar setting for Taobao by allowing it to access her location information exclusively when she was using the application. As highlighted by Interviewee 24, "Because these platforms have already penetrated into each aspect of our life, it is very difficult to refuse to use this platform completely. But we can try to set as many protective functions as possible." Therefore, besides these settings, Interviewee 24 also adjusted her approach to posting content on WeChat. When sharing a WeChat Moment,[9] she "firstly set the groups [of people who can view], and then set up the [time] limited access [for the post and moment function]."

## Comparisons Between the PIPL, the Platforms, and the Users

### *The Synergistic Actions of the State, Law, and Policy*

"This Law is enacted in accordance with the Constitution for the purposes of protecting the rights and interests on personal information, regulating personal information processing activities, and promoting reasonable use of personal information" (PIPL, 2021). This is Article 1 of the PIPL, which introduced its general provisions. By establishing the PIPL as a "family" resemblance with the Western information protection regime, the law granted platforms specific rights related to privacy protection (Creemers, 2022). Interviewee 11 commented that "the national promulgation of the PIPL is a necessary step in the current social environment because personal privacy has been under discussion for many years, and this marks the first step." This robust state governance necessitated a response from these digital platforms that led to their synergistic actions in formulating, updating, and communicating platform privacy policies. This, in turn, resulted in the users developing various perceptions and reactive behaviors toward these privacy practices. The actions taken by the platforms and the reactions displayed by the users exemplified a top-down approach that emphasized adherence to the legal requirements set forth by the state. The PIPL was the driving force behind this process, which can be observed by utilizing the platforms as the agents to balance national interests and individual privacy rights.

### *Divergent Privacy Practices Between Platforms and Users*

While the platforms strived to establish, update, and enhance their privacy policies and related practices under the supervision of the PIPL by implementing standardized notification models, granting user rights for information management, safeguarding user information through utilization and protection measures, and justification of data ownership, these actions have resulted in a series of privacy practices that diverge from users' interests. Interviewee 4 explained this divergence by saying that the "platforms used to not have my complete information, but now they can use their regulations to achieve this goal without undertaking any obligations." In contrast, the users tend to overlook fundamental privacy concerns, such as the surveillance of user data and behavior and

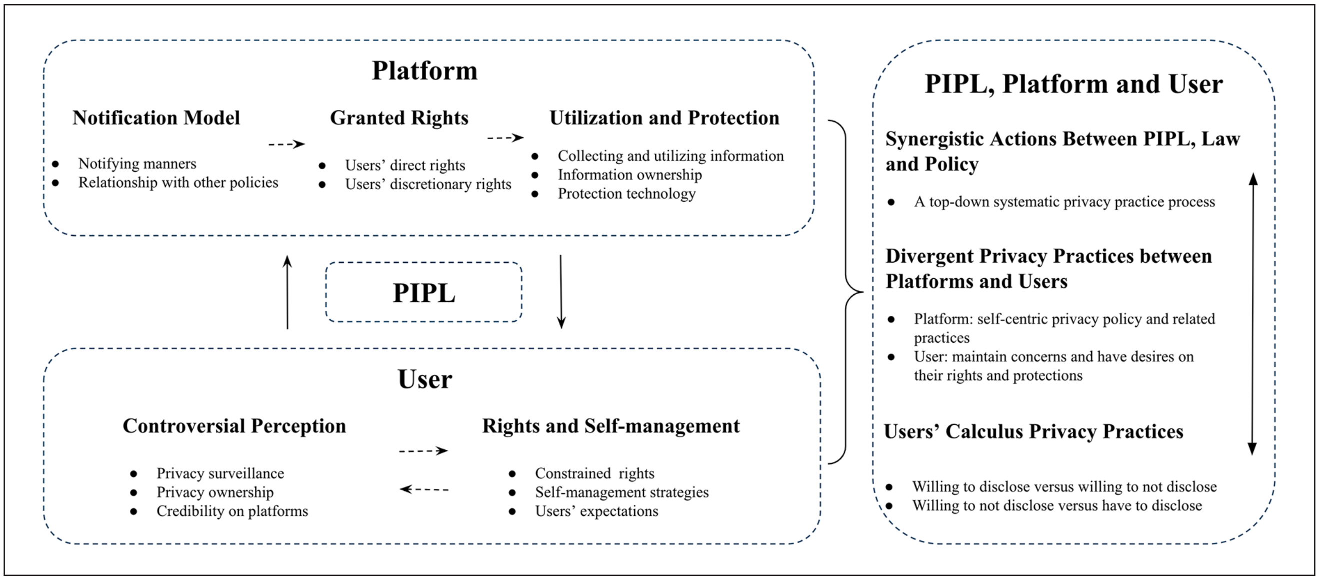

Platform
Notification Model
Notifying manners
Relationship with other policies
Granted Rights
Users' direct rights
Users' discretionary rights
Utilization and Protection
Collecting and utilizing information
Information ownership
Protection technology
PIPL
User
Controversial Perception
Privacy surveillance
Privacy ownership
Credibility on platforms
Rights and Self-management
Constrained rights
Self-management strategies
Users' expectations
PIPL, Platform and User
Synergistic Actions Between PIPL, Law and Policy
A top-down systematic privacy practice process
Divergent Privacy Practices between Platforms and Users
Platform: self-centric privacy policy and related practices
User: maintain concerns and have desires on their rights and protections
Users' Calculus Privacy Practices
Willing to disclose versus willing to not disclose
Willing to not disclose versus have to disclose

**Figure 4.** A triple-layered comparative privacy analytical framework.

the lack of complaint mechanisms when user privacy is threatened. However, these concerns are not addressed by the platforms, which are seen to solely fulfill the requirements stipulated by the PIPL while disregarding their users' aforementioned privacy concerns.

### *Users' Calculus Privacy Practices*

The users expressed concerns during the interviews regarding the rights granted by the platforms and their privacy practices, irrespective of the state's involvement. Interviewee 24 emphasized her trust in the government due to its vigilance toward "the potential information security issues" on the platforms, particularly considering that "the government also utilizes these platforms and their data for national security purposes." However, the implementation of new privacy measures under the PIPL framework did not effectively enhance the users' sense of security toward the platforms but rather heightened their apprehensions about privacy. As Interviewee 17 claimed,

> I have to agree because I need to use it. Anyway, I can do nothing, update [policies] or not, agree [policies] or not, if this app wants your privacy, there is nothing I can do. So, I don't feel safe because for most people in this digital world, we are actually transparent. There is actually no privacy to a certain extent.

The interviews also revealed that users often weighed the benefits and risks before disclosing personal information. The users described China's platforms as exerting significant influence over their daily lives to the extent that they felt compelled to divulge personal information because "these platforms must be used every day" (Interviewee 26). This led to varying reactions among the users regarding the self-management of their personal privacy. In contrast to those who actively engaged in privacy management, many employed the platform settings to manually restrict access to their private information, adjusted their content production strategies, and even created multiple accounts to safeguard their privacy. However, these varied practices of privacy calculus among users highlight the need for privacy literacy and the trade-off between privacy and convenience in managing their personal information. This further positioned them as subjects subjected to an ongoing asymmetric relationship with the platforms.

Therefore, based on these findings, we have developed a triple-layered comparative privacy research approach (see Figure 4): (1) examining platform responses to the PIPL in terms of notifications, granted rights, and information utilization and protection; (2) investigating users perceptions and self-management of privacy as influenced by the platforms under the PIPL guidance; (3) understanding the interconnections and divergences among PIPL, platforms, and users. This framework provides a potential avenue for future research aimed at clarifying the multidimensionalities, complexities, commonalities, and discrepancies inherent in privacy practices governed by state law, digital platforms, privacy policies, and users.

## Discussion

The triple-layered comparative approach utilized in this study revealed the polarized reactions of platform users to the privacy policy issues that emerged subsequent to the implementation of the PIPL in China. Our research demonstrated that the three platforms have employed distinct discursive strategies—retrospective analysis, data localization, and technology authorization to formulate and communicate their privacy policies, yet they all articulate their legitimacy and authority over users' private data as a shared objective. Nevertheless, these legitimized discursive strategies significantly undermine users' ownership of personal digital assets. Consequently, these platforms have prioritized their own interests over the protection of users by adopting a responsive approach to defining and managing users' personal information. It is imperative for platforms to address how such sensitive information is stored and protected to uphold and legitimize their role as privacy regulators. Given the inherent dominant power of the platforms, users tend to position themselves as passive and powerless in defending their privacy and comprehending new privacy policies. Thus, we conclude that the in-progress hegemonic monopoly of the platforms may contribute to the limited domestication of privacy literacy of daily users.

Moreover, despite the enforcement mechanisms of the post-PIPL privacy policies, user-oriented privacy issues and concerns remain unresolved due to their inadequate agency in exercising their privacy rights. The establishment of self-protection and self-determination literacies has not been effectively achieved (Masur, 2020). In addition, simply pointing to privacy practices and regulations as key sources of the party's governance and state surveillance in China fails to account for user agency, the platforms' innovation, and the national (counter-)narratives in the global race for technological supremacy in privacy. By examining the asymmetrical power dynamics between platforms and users in the PIPL context, we define the new privacy policies as a digital formalism resembling Skyloft-like practices.

Furthermore, the comparative privacy research framework as a theoretical perspective guide (Masur et al., 2021) is applicably expanded into this empirical study. The logic that underpins digital privacy practices in China involves multilevel power dynamics within a patriarchal management system, one that includes political interactions between the platforms and the state, cultural and power dynamics between platforms and users, and the influence of technology on user behaviors. Compared with previous Western-centric privacy studies, our study enriches the understanding of digital privacy policies by providing multifaceted perspectives within a dynamic process influenced by national interests and intertwined with authoritarian state regulations, commercial institutions, and online consumer behaviors. Through echoing the previous literature to incorporate privacy concerns specific to China and the PIPL contexts, this study contributes practical knowledge of privacy protection models to the ongoing academic discourse. This can be considered a praxis approach to understanding non-Western digital privacy policies that significantly affect data regulatory strategies in the Global South and reshape data governance for transnational enterprises headquartered in China (Calzada, 2022; Jin & Skiera, 2022).

The findings indicate that digital platform privacy practices and user perceptions primarily lay in safeguarding commercial rights rather than engaging in a comprehensive discussion on "personal information" at the national and governmental levels. This result echoes the essence of the PIPL, which acknowledges the distinctive characteristics of personal information compared to Western norms. In China, individual rights are inherently interconnected with and linked to the party, state, and collective (Douglas, 2000). Consequently, privacy practices and protection primarily reinforce the state's ideology by regarding privacy rights as matters of national security and commercial interests (Moreira, 2023) rather than the individual rights of citizens aimed at constraining relevant governing authorities. However, the introduction of the PIPL and the platforms' updated privacy policies mark a significant milestone in personal information governance. These developments also serve as a valuable reference for describing non-Western and developing countries' practices, as the PIPL is positioned as an innovative third model of privacy governance beyond the GDPR and the CCPA (Pernot-Leplay, 2020). Furthermore, these PIPL-driven privacy measures can be interconnected with the GDPR and the CCPA to develop a practical framework for comprehending global privacy governance.

## Conclusion

This study delineates the complex power dynamics between digital platforms, their privacy policies, and users by employing a triple-layered comparative approach to investigate privacy issues based on empirical evidence. It conducts a nuanced analysis that can inform governments and platforms as they implement and optimize privacy-related policies. Importantly, our research provides timely practical insights into the PIPL-based privacy policies as supplementary measures for digital privacy practices in the Global South. However, the case study is limited by its exclusive focus on prominent Chinese platforms while excluding less-used platforms, such as those related to health or tourism services. Ultimately, we suggest that future research can investigate the shifts in the discourses related to privacy practices with a broad selection of different types of platforms, as well as Chinese and overseas versions, thereby contributing to establishing a practical framework of global digital privacy derived from Chinese experiences.

### Author's Note

The identities of the interviewees involved in the article have been anonymized to ensure their confidentiality and protect their privacy.

### Acknowledgements

We extend our sincere gratitude to the anonymous reviewers and editorial team for their invaluable feedback and greatly appreciate the support of all interviewees involved in this study. During the preparation of this work, the author(s) used Grammarly to check and improve the language. The author(s) reviewed and edited the content as needed and take(s) full responsibility for the publication's content.

## Author Contributions

L.L. collected data and drafted the initial article, while Y.C. designed the entire study and methdology, collected partial data, and rewrote the article. Both authors contributed to revising and approving the final version of the article.

## Consent to Participate

All participants were provided with comprehensive information regarding this study and underwent a process of informed consent through written documentation.

## Consent for Publication

The author has obtained the necessary written informed consent for the publication of this research.

## Data Availability

See the "Notes" section of the article for access to the public data regarding privacy laws and policies.

## Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

## Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

## Ethical Approval

This research has been approved by the Office of Research Ethics at the Xi'an Jiaotong Liverpool University (Approval Number: ER-LRR-11000146420231109133156)

## ORCID iDs

Liming Liu https://orcid.org/0000-0001-8873-3097
Yiming Chen https://orcid.org/0000-0003-2789-5468

## Notes

1. See, Personal Information Protection Law (PIPL) was adopted at the 30th Meeting of the Standing Committee of the Thirteenth National People's Congress on 20 August 2021. PIPL's English translation version was last updated on 29 December 2021. http://en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559.htm
2. General Data Protection Regulation (GDPR). Available online: www.gdpr-info.eu (accessed on 15 January 2024).
3. California Consumer Privacy Act (CCPA). Available online: https://www.oag.ca.gov/privacy/ccpa (accessed on 15 January 2023).
4. National People's Congress. Data Security Law of the People's Republic of China, 2021. https://digichina.stanford.edu/work/translation-data-security-law-of-the-peoples-republic-of-china/ (accessed on 11 July 2022).
5. Taobao App is an e-commerce platform that enables users to purchase products directly from vendors in China.
6. WeChat is a multifunctional Chinese mobile application that integrates instant messaging, social media, and mobile payment services.
7. Douyin, the domestic version of TikTok, is a service platform for short-form videos.
8. The privacy policies used in this study are from 2022 and have been saved by the authors. The product's website may regularly update these policies. WeChat privacy policy: https://www.wechat.com/zh_CN/privacy_policy.html. Taobao privacy policy: https://terms.alicdn.com/legal-agreement/terms/suit_bu1_taobao/suit_bu1_taobao201703241622_61002.html. Douyin privacy policy: https://www.douyin.com/draft/douyin_agreement/douyin_agreement_privacy.html?id=6773901168964798477
9. Moment is a key function for sharing user life on WeChat, akin to Facebook's "moments" feature.

## References

Antón, A. I., Earp, J. B., He, Q., Stufflebeam, W., Bolchini, D., & Jensen, C. (2004). Financial privacy policies and the need for standardization. *IEEE Security & Privacy*, *2*(2), 36–45.

Avancha, S., Baxi, A., & Kotz, D. (2012). Privacy in mobile technology for personal healthcare. *ACM Computing Surveys (CSUR)*, *45*(1), 1–54.

Bonneau, J., & Preibusch, S. (2010). The privacy jungle: On the market for data protection in social networks. In T. Moore, D. Pym, & C. Ioannidis (Eds.), *Economics of information security and privacy* (pp. 121–167). Springer.

Calzada, I. (2022). Citizens' data privacy in China: The state of the art of the Personal Information Protection Law (PIPL). *Smart Cities*, *5*(3), 1129–1150.

Cao, J. (2005). Protecting the right to privacy in China. *Victoria University of Wellington Law Review*, *36*, 645–664.

Capurro, R. (2005). Privacy. An intercultural perspective. *Ethics and Information Technology*, *7*, 37–47.

Chen, Z. T., & Cheung, M. (2018). Privacy perception and protection on Chinese social media: A case study of WeChat. *Ethics and Information Technology*, *20*(4), 279–289.

Choi, H., Park, J., & Jung, Y. (2018). The role of privacy fatigue in online privacy behavior. *Computers in Human Behavior*, *81*, 42–51.

Citron, D. K. (2019). Sexual privacy. *The Yale Law Journal*, *128*(7), 1870–1960.

Creemers, R. (2022). China's emerging data protection framework. *Journal of Cybersecurity*, *8*(1), 1–12.

Crémer, J., De Montjoye, Y.-A., & Schweitzer, H. (2019). *Competition policy for the digital era*. European Commission.

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science*, *10*(1), 104–115.

Dal, A. (2024). Firewalls have ears: How horizontal privacy regulation influences online political expression in Russia. *International Journal of Communication*, *18*, 2731–2752.

De Leyn, T., Waeterloos, C., De Wolf, R., Vanhaelewyn, B., Ponnet, K., & De Marez, L. (2022). Teenagers' reflections on media literacy initiatives at school and everyday media literacy discourses. *Journal of Children and Media*, *16*(2), 221–239.

Diaz, C., & Gürses, S. (2012). Understanding the landscape of privacy technologies. *Proceedings of the Information Security Summit*, *12*, 58–63.

Douglas, E. E. (2000). The struggle for human rights versus stability: The Chinese Communist Party and Western values clash. *Denver Journal of International Law & Policy*, *29*, 151.

Duguay, S., Dietzel, C., & Myles, D. (2024). The year of the "virtual date": Reimagining dating app affordances during the COVID-19 pandemic. *New Media & Society*, *26*(3), 1384–1402.

Esser, F., & Hanitzsch, T. (2013). On the why and how of comparative inquiry in communication studies. In F. Esser & T. Hanitzsch (Eds.), *The handbook of comparative communication research* (pp. 25–44). Routledge.

Fairclough, N., & Wodak, R. (1997). Critical discourse analysis. In T. A. van Dijk (Ed.), *Discourse as social interaction* (pp. 258–284). SAGE.

Feng, J. (2019). Party regulations and State Laws in China: A disappearing boundary and growing tensions. *Chinese Law & Government*, *51*(5–6), 260–276.

Fenton, N., Freedman, D., Schlosberg, J., & Dencik, L. (2020). *The media manifesto*. John Wiley.

Ferris, L., & Duguay, S. (2020). Tinder's lesbian digital imaginary: Investigating (im) permeable boundaries of sexual identity on a popular dating app. *New Media & Society*, *22*(3), 489–506.

Gao, Y., & Xu, J. (2022, June 8). Unclear supervisors behind app personal information protection. *DeHeng Law Offices*. https://www.dehenglaw.com/CN/tansuocontent/0008/025360/7.aspx?MID=0902

Gossart, C. (2014). Can digital technologies threaten democracy by creating information cocoons? In J. Bishop (Ed.), *Transforming politics and policy in the digital age* (pp. 145–154). IGI Global.

Greene, D., & Shilton, K. (2018). Platform privacies: Governance, collaboration, and the different meanings of "privacy" in iOS and Android development. *New Media & Society*, *20*(4), 1640–1657.

Greenleaf, G. (2021). *China's completed Personal Information Protection Law: Rights plus cyber-security* (172 Privacy Laws & Business International Report 20-23 No. 21-91; UNSW Law Research Paper). https://doi.org/10.2139/ssrn.3989775

Haim, M., Graefe, A., & Brosius, H.-B. (2018). Burst of the filter bubble? Effects of personalization on the diversity of Google News. *Digital Journalism*, *6*(3), 330–343.

Huckvale, K., Torous, J., & Larsen, M. E. (2019). Assessment of the data sharing and privacy practices of smartphone apps for depression and smoking cessation. *JAMA Network Open*, *2*(4), e192542.

Ibdah, D., Lachtar, N., Raparthi, S. M., & Bacha, A. (2021). "Why should I read the privacy policy, I just need the service": A study on attitudes and perceptions toward privacy policies. *IEEE Access*, *9*, 166465–166487.

Jia, K., Kenney, M., Mattila, J., & Seppala, T. (2018). *The application of artificial intelligence at Chinese digital platform giants: Baidu, Alibaba and Tencent* (No. 81; ETLA Report). The Research Institute of the Finnish Economy.

Jiang, J., & Zheng, Z. (2023). Personal information protection and privacy policy compliance of health code apps in China: Scale development and content analysis. *JMIR mHealth and uHealth*, *11*, e48714.

Jin, Y., & Skiera, B. (2022). How do privacy laws impact the value for advertisers, publishers and users in the online advertising market? A comparison of the EU, US and China. *Journal of Creating Value*, *8*(2), 306–327.

Kai, Q., & Zhou, Z. (2022). Global digital governance: Progress, dilemmas and China's role. *China International Studies*, *97*, 5.

Kang, H., & Oh, J. (2023). Communication privacy management for smart speaker use: Integrating the role of privacy self-efficacy and the multidimensional view. *New Media & Society*, *25*(5), 1153–1175.

Li, H. (2020). Negotiating privacy and mobile socializing: Chinese university students' concerns and strategies for using geosocial networking applications. *Social Media+ Society*, *6*(1), 2056305120913887.

Light, B., Burgess, J., & Duguay, S. (2018). The walkthrough method: An approach to the study of apps. *New Media & Society*, *20*(3), 881–900.

Liu, K., Xu, G., Zhang, X., Xu, G., & Zhao, Z. (2022). Evaluating the privacy policy of Android apps: A privacy policy compliance study for popular apps in China and Europe. *Scientific Programming*, *2022*, 2508690.

Liu, Y. L., Huang, L., Yan, W., Wang, X., & Zhang, R. (2022). Privacy in AI and the IoT: The privacy concerns of smart speaker users and the Personal Information Protection Law in China. *Telecommunications Policy*, *46*(7), 102334.

Liu, Y. L., Yan, W., & Hu, B. (2021). Resistance to facial recognition payment in China: The influence of privacy-related factors. *Telecommunications Policy*, *45*(5), 102155.

Liu, Y. L., Yan, W., Hu, B., Lin, Z., & Song, Y. (2024). Chatbots or humans? Effects of agent identity and information sensitivity on users' privacy management and behavioral intentions: A comparative experimental study between China and the United States. *International Journal of Human-Computer Interaction*, *40*(19), 5632–5647.

Marwick, A. E., & Boyd, D. (2014). Networked privacy: How teenagers negotiate context in social media. *New Media & Society*, *16*(7), 1051–1067.

Masur, P. K. (2018). *Situational privacy and self-disclosure: Communication processes in online environments*. Springer.

Masur, P. K. (2020). How online privacy literacy supports self-data protection and self-determination in the age of information. *Media and Communication*, *8*(2), 258–269.

Masur, P. K., Epstein, D., Quinn, K., Wilhelm, C., Baruh, L., & Lutz, C. (2021). A comparative privacy research framework. *SocArXiv*. https://doi.org/10.31235/osf.io/fjqhs

Matamoros-Fernández, A. (2017). Platformed racism: The mediation and circulation of an Australian race-based controversy on Twitter, Facebook and YouTube. *Information, Communication & Society*, *20*(6), 930–946.

Moreira, H. (2023, January 30). *Governing knowledge and technology: Technological pressure for convergence in EU, California, and China data protection regulation*. https://doi.org/10.31235/osf.io/v6uf3

Pangrazio, L., & Selwyn, N. (2019). 'Personal data literacies': A critical literacies approach to enhancing understandings of personal digital data. *New Media & Society*, *21*(2), 419–437.

Park, Y. J., & Jang, S. M. (2014). Understanding privacy knowledge and skill in mobile communication. *Computers in Human Behavior*, *38*, 296–303.

Pekárek, M., & Pötzsch, S. (2009). A comparison of privacy issues in collaborative workspaces and social networks. *Identity in the Information Society*, *2*, 81–93.

Pernot-Leplay, E. (2020). China’s approach on data privacy law: A third way between the US and the EU? *Penn State Journal of Law & International Affairs*, *8*, 49.

Personal Information Protection Law. (2021). *Personal information protection law of the People’s Republic of China*. The National People’s Congress of the People’s Republic of China. http://en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559.htm

Proctor, R. W., Ali, M. A., & Vu, K.-P. L. (2008). Examining usability of web privacy policies. *International Journal of Human-Computer Interaction*, *24*(3), 307–328.

Richards, N. M., & Solove, D. J. (2010). Prosser’s privacy law: A mixed legacy. *California Law Review*, *98*, 1887–1924.

Rössler, B. (2005). *The value of privacy*. Polity Press.

Shen, X. (2018, March 28). Chinese internet users criticize Baidu CEO for saying people in China are willing to give up data privacy for convenience. *South China Morning Post*. https://www.scmp.com/abacus/tech/article/3028402/chinese-internet-users-criticize-baidu-ceo-saying-people-china-are

Su, C., & Flew, T. (2021). The rise of Baidu, Alibaba and Tencent (BAT) and their role in China’s Belt and Road Initiative (BRI). *Global Media and Communication*, *17*(1), 67–86.

Tan, Z., & Zhang, C. (2021). China’s PIPL and DSL: Is China following the EU’s approach to data protection? *Journal of Data Protection & Privacy*, *5*(1), 7–25.

Trepte, S., & Masur, P. K. (2016). *Cultural differences in social media use, privacy, and self-disclosure: Research report on a multicultural study*. University of Hohenheim.

Trepte, S., Teutsch, D., Masur, P. K., Eicher, C., Fischer, M., Hennhöfer, A., & Lind, F. (2015). Do people know about privacy and data protection strategies? Towards the “Online Privacy Literacy Scale” (OPLIS). In S. Gutwirth, R. Leenes, & P. de Hert (Eds.), *Reforming European data protection law* (pp. 333–365). Springer.

Van Hoboken, J., & Fathaigh, R. Ó. (2021). Smartphone platforms as privacy regulators. *Computer Law & Security Review*, *41*, 105557.

Wang, H. (2011). *Protecting privacy in China*. Springer.

Wang, Z., & Yu, Q. (2015). Privacy trust crisis of personal data in China in the era of Big Data: The survey and countermeasures. *Computer Law & Security Review*, *31*(6), 782–792.

Wodak, R., & Meyer, M. (2009). Critical discourse analysis: History, agenda, theory, and methodology. In R. Wodak & M. Meyer (Eds.), *Methods of critical discourse analysis* (pp. 1–33). SAGE.

Xu, K., Liu, V., Luo, Y., & Yu, Z. (2021, August 24). Analyzing China’s PIPL and how it compares to the EU’s GDPR. *The International Association of Privacy Professionals*. https://iapp.org/news/a/analyzing-chinas-pipl-and-how-it-compares-to-the-eus-gdpr/

Yang, H., & Liu, H. (2014). Prior negative experience of online disclosure, privacy concerns, and regulatory support in Chinese social media. *Chinese Journal of Communication*, *7*(1), 40–59.

You, C. (2022). Half a loaf is better than none: The new data protection regime for China’s platform economy. *Computer Law & Security Review*, *45*, 105668.

Zhu, J. (2022, February 14). The Personal Information Protection Law: China’s version of the GDPR? *Columbia Journal of Transnational Law*. https://www.jtl.columbia.edu/bulletin-blog/the-personal-information-protection-lawchinas-version-of-the-gdpr

Zhu, Y. (2022). Social media and state surveillance in China: The Interplay between authorities, businesses and citizens. In E. Celeste, A. Heldt, & C. I. Keller (Eds.), *Constitutionalising social media* (pp. 199–216). Bloomsbury Publishing.

## Author Biographies

Liming Liu (MA, Uppsala University) is a PhD student in Communication at the Hugh Downs School of Human Communication, Arizona State University. His research interests include the socio-cultural implications of emerging technologies and digital media studies, with a specialization in privacy practices of social media and human–AI communication in a digital era.

Yiming Chen (PhDs, Uppsala University/Vrije Universiteit Brussel) is an Assistant Professor at the Academy of Film and Creative Technology, Xi’an Jiaotong-Liverpool University. His research interests focus on critically exploring complex relationships between platform policies of social media, technology practices, and content creation.