Understanding Chinese Internet Users' Perceptions of, and Online Platforms' Compliance with, the Personal Information Protection Law (PIPL)

MORGANA MO ZHOU, City University of Hong Kong, China
ZHIYAN QU, City University of Hong Kong, China
JINHAN WAN, City University of Hong Kong, China
BO WEN, University of Macau, China
YAXING YAO, Virginia Tech, USA
ZHICONG LU, City University of Hong Kong, China

The Personal Information Protection Law (PIPL) was implemented in November 2021 to safeguard the personal information rights and interests of Internet users in China. However, the impact and existing shortcomings of the PIPL remain unclear, carrying significant implications for policymakers. This study examined privacy policies on 13 online platforms before and after the PIPL. Concurrently, it conducted semi-structured interviews with 30 Chinese Internet users to assess their perceptions of the PIPL. Users were also given tasks to identify non-compliance within the platforms, assessing their ability to address related privacy concerns effectively. The research revealed various instances of non-compliance in post-PIPL privacy policies, especially concerning inadequate risk assessments for sensitive data. Although users identified some non-compliant activities like app eavesdropping, issues related to individual consent proved challenging. Surprisingly, over half of the interviewees believed that the government could access their personal data without explicit consent. Our findings and implications can be valuable for lawmakers, online platforms, users, and future researchers seeking to enhance personal privacy practices both in China and globally.

CCS Concepts: • **Security and privacy** → **Privacy protections**; • **Human-centered computing** → *Empirical studies in HCI*.

Additional Key Words and Phrases: Personal Information Protection Law, Informed Consent, Users' Perception, Chinese Law, Qualitative Methods

ACM Reference Format:
Morgana Mo Zhou, Zhiyan Qu, Jinhan Wan, Bo Wen, Yaxing Yao, and Zhicong Lu. 2024. Understanding Chinese Internet Users' Perceptions of, and Online Platforms' Compliance with, the Personal Information Protection Law (PIPL). *Proc. ACM Hum.-Comput. Interact.* 8, CSCW1, Article 138 (April 2024), 26 pages. https://doi.org/10.1145/3637415

Authors' addresses: Morgana Mo Zhou, mzhou25-c@my.cityu.edu.hk, City University of Hong Kong, Tat Chee Avenue, Hong Kong, China; Zhiyan Qu, zhiyanqu2-c@my.cityu.edu.hk, City University of Hong Kong, Tat Chee Avenue, Hong Kong, China; Jinhan Wan, jinhanwan2-c@my.cityu.edu.hk, City University of Hong Kong, Tat Chee Avenue, Hong Kong, China; Bo Wen, bowen@um.edu.mo, University of Macau, Avenida da Universidade, Taipa, Macau, China, 999078; Yaxing Yao, yaxing@vt.edu, Virginia Tech, 925 Prices Fork Road, Blacksburg, Virginia, USA, 24061-0002; Zhicong Lu, zhiconlu@cityu.edu.hk, City University of Hong Kong, Tat Chee Avenue, Hong Kong, China.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.
© 2024 Copyright held by the owner/author(s). Publication rights licensed to ACM.
2573-0142/2024/4-ART138 $15.00
https://doi.org/10.1145/3637415

1 INTRODUCTION

With the widespread availability of smartphones and mobile Internet, users have come to rely on online platforms and applications for everything from business transactions and communication to transportation and entertainment [9, 15]. As such online platforms provide highly tailored, personalized services, they often utilize vast amounts of personal information such as fingerprints, facial data, financial details, and users' locations [24, 29, 40]. The collection of such data has raised significant privacy concerns, given the extensive access that such online platforms have to users' personal information [24, 60]. Recently, there have been instances where online platforms have collected and used user data without the informed consent of, or proper disclosure to, users. For example, in July 2022, Didi, the Chinese equivalent of Uber, was fined CNY 8 billion (USD 1.2 billion) for excessively collecting and unlawfully processing 64.7 billion personal data [46].

The need to protect individuals' privacy has thus been a focal point of the legislation introduced in many regions and countries [24]. In Europe, for example, the General Data Protection Regulation (GDPR) regulates the collection and handling of personal information and provides enhanced privacy protection across various sectors, such as financial markets, Internet of Things devices, and healthcare [2, 13, 17, 35, 49]. Following the implementation of GDPR, Europe saw a significant decline in privacy-invasive issues [53].

Other regions and countries have also taken steps to enact their own data and privacy protection laws. For example, in China, the Personal Information Protection Law (PIPL) of the People's Republic of China was approved in August 2021 [47] and invoked in November 2021. The PIPL aimed to protect personal information rights, standardize information handling practices, specify comprehensive and rigorous provisions regarding informed user consent, and promote the responsible use of personal data [47]. The PIPL is the first legislation specifically designed to safeguard personal information and address the prevalent privacy concerns across numerous online platforms [11, 12, 16, 45]. Since its implementation in November 2021, the Chinese government has taken decisive measures to address illegal activities relating to personal information protection, while online platforms operating in China have made operational adjustments to ensure that they are compliant with PIPL's requirements [3, 11].

Prior to the invocation of PIPL, the legislative landscape in China was fragmented and provided inadequate protection for individuals' rights [70]. The PIPL represented an important step towards enhancing the privacy ecosystem in China and could be a valuable tool to mitigate the prevalent privacy infringements in the country [11]. However, the degree to which compliance with the PIPL has resulted in increased privacy protections for Chinese citizens is currently unknown. Further, as many of the non-compliant activities that online platforms can exhibit can pose substantial threats to user privacy (e.g., unauthorized access to personal information), users' abilities to identify and perceive such activities play a crucial role when deciding whether to use an online platform. Guided by these concerns, this research sought to answer the following research questions:

- **RQ1:** What has the effect of the PIPL been on personal information protection and online platforms' compliance?
- **RQ2:** Can users recognize non-compliant activities in privacy policies?
- **RQ3:** What are users' perceptions towards these non-compliant activities?

An analysis of the privacy policies of 13 popular online platforms in China, such as WeChat, QQ, and Douyin, was conducted to answer these research questions. The analysis compared the privacy policies before and after the PIPL was invoked to identify any significant changes that resulted. This process identified different types of non-compliance activities within post-PIPL privacy policies, including the absence of personal information risk assessments for handling sensitive data, inconvenient consent revocation processes, and insufficient measures to separate the notification and acquisition of individual consent. To gain insights into users' abilities to recognize non-compliant activities and understand their perceptions of these activities, semi-structured interviews were conducted with 30 Chinese Internet users who actively engaged with the 13 platforms. These interviews highlighted how interviewees could identify non-compliant activities such as app eavesdropping and the excessive collection of personal information. However, they struggled to identify non-compliant activities related to individuals' separate consent. Moreover, approximately half of the interviewees believed the government should collect and handle their personal information without explicit consent.

This research thus makes several contributions to HCI and CSCW, including:

- A summary of the changes and instances of non-compliant activities observed in the privacy policies of 13 popular online platforms in China.
- An identification of the challenges faced by laypersons when comprehending PIPL and verifying platform compliance.
- An uncovering of the privacy concerns specific to the Chinese cultural context, e.g., Chinese Internet users were more concerned with information leakage rather than whether their data was being collected and stored.
- Recommendations for lawmakers, personal information processors, users, and future researchers to enhance personal information practices in China and worldwide.

2 PERSONAL INFORMATION PROTECTION LAW (PIPL)

Effective November 2021, PIPL was China's first law specifically designed to protect personal information [47]. The purposes of PIPL were to secure personal information rights and interests and regulate the rules governing the processing and utilization of personal information [7, 44].

The PIPL defined *personal information* as "various kinds of information related to identified or identifiable natural persons recorded by electronic or other means, excluding the information processed anonymously (Article 4)" [47]. It stated *the processing of personal information*, including "collection, storage, use, processing, transmission, provision, publication, and erasure of personal information (Article 4)" [47]. Personal information processing activities only occurred under special legal circumstances, for example, after receiving consent from the data's user, collecting information related to public health emergencies, the information exposed by data subjects themselves, and so on (Article 13). Similar to GDPR, PIPL applied the data minimization principle to personal information processing activities to restrict a personal information processor from collecting unnecessary and unauthorized personal information (Article 6). The data minimization principle was that "collection of personal information shall be limited to the minimum scope for processing and excessive collection of personal information shall not be allowed (Article 6)" [47]. The PIPL also specified special information collection rules, including those on sensitive personal information processing and the processing of personal information by the government (Section 2, 3, Chapter II). Sensitive personal information was considered to be information that would lessen one's reputation or personal and property security (Article 28). As PIPL also considered all information related to children under 14 years of age as sensitive information, if a personal information processor wanted to utilize such data, it needed to acquire consent from the children's parents or guardians (Article 31). For state organs, PIPL enabled such entities to gather and use personal information as needed without consent.

PIPL also introduced user privacy rights, for example, the right to be informed, the right to reject personal information processing activities, the right for a user to inquire and copy their personal information from a relevant personal information processor, and the right to correct or delete one's personal information. Furthermore, during personal information processing activities, PIPL enabled users to withdraw their consent from a personal information processor during consent-based processing activities (Article 15). If automated decision-making significantly impacted users' profits and interests, PIPL permitted users to reject automated decision-making or acquire a comprehensive explanation from the personal information processor (Article 24).

3 RELATED WORK

Of most relevance to the present research is the literature on the degree to which online platforms complied with GDPR, users' privacy concerns, and their perceptions about personal information protection laws within the context of GDPR, and attitudes and concerns about privacy held by non-Western users.

3.1 Compliance with GDPR

GDPR has been regarded as an efficient tool to protect users' data [5], and it has been believed that good compliance with GDPR would decrease privacy-invasive problems and improve privacy environments [53]. Previous studies have made efforts to understand the degree to which privacy policies are compliant with GDPR [4, 6, 18, 30, 39, 43, 63] and many researchers have found several non-compliance issues [18, 39, 43, 63]. For example, Mohan et al. found several general GDPR non-compliance activities that occurred on large-scale cloud services when analyzing the privacy policies of cloud services after GDPR was published [43]. Moreover, Kyi et al. focus on the ambiguous design and description in privacy policies, they summarized the deceptive strategies used in privacy notices, such as hiding legitimate privacy information at the end of privacy policies, using complicated procedures to revoke one's permission after it had been granted for access by the data processor, and the use of linguistic tricks when writing privacy policies, such as providing an implicit definition of legitimate interests to users or even do not give any specific explanation [34]. They also found that non-compliant platforms had ambiguous data processing and sharing rules, mentioned a few explicit durations that they would maintain users' personal information, and used inappropriate methods to alert users about privacy policy updates, thus providing users with little power to control their data. Fan et al. explored the common situations in that data processors violated the GDPR, they summarized three GDPR requirements for protecting users' personal information that were violated by personal information processors [18], i.e., they provided insufficient data processing records to users, they obtained user data in excess of what was declared in their privacy policies. Moreover, they lacked appropriate security approaches to protect users' personal information. Bowyer et al. also highlighted the difficulties that users had when attempting to access their personal information, such as insufficient transparency on information handling and transportation and confusing information on the personal data that could be exported [5].

To improve compliance with GDPR, researchers have also explored the design of innovative systems to provide better enforcement [1, 8, 62, 67, 68]. Campanile et al., for example, proposed a reference model to manage the information within the Internet of Vehicles, such as locations and personal habits, utilizing block-chains [8].

The research above provided evidence that non-compliance activities still exist, even after the invocation of GDPR. Similarly, we assumed that the same situation occurred after the invocation of PIPL, so we analyzed the most popular Chinese online platforms' privacy policies to determine their degree of compliance with PIPL.

3.2 Western Attitudes Towards GDPR

Current research has explored personal information protection laws, especially since the introduction of GDPR. When GDPR was first implemented in Europe, researchers explored GDPR's execution and impact [37, 55] in fields such as healthcare [21, 35], the Internet of Things [49, 64], and the economy [2]. As GDPR aimed to protect users' privacy, a large amount of research explored users' perceptions and awareness of GDPR and which GDPR regulations were connected to privacy concerns [19, 32, 41, 50, 51]. For example, Tahal and Formanek investigated attitudes towards GDPR from the perspective of Czech Republic citizens [61]. In their study, participants thought that GDPR was mostly helpful but somewhat annoying, and they doubted that GDPR could affect data processing. Strycharz et al. conducted a survey of 1288 users in the Netherlands to explore their understanding of GDPR and its aims and gather their reactions to GDPR [59]. The results showed that most users had a high awareness of GDPR and individual rights. However, they questioned the effectiveness of GDPR with respect to individual rights. Furthermore, González et al. noted that there were six dimensions of GDPR that were associated with users' privacy concerns, i.e. data collection, data handling and storage, ownership agency, privacy and security items, security mechanisms, and privacy and security risks [22].

Previous researchers have made efforts to understand various aspects of GDPR for protecting users' privacy, including GDPR's implementation and impact and users' perception and awareness of GDPR. Similar as GDPR, the PIPl is also the law protecting users' privacy information. Moreover, the PIPL is the first official and legal law to protect users' information in China. Therefore, PIPL has a noticeable influence on Chinese society and industry. Furthermore, China has almost 1.4 billion population in the world, which is 20% of the world population. Therefore, we are motivated to investigate PIPL's implementation and impact and Chinese citizens' perceptions and awareness of PIPL in this research.

3.3 Non-Western Privacy Concerns

Non-Western Privacy Concerns occupy a central role in the complex landscape of online privacy attitudes and behaviors. While much research has focused on Western users, few studies have delved into the distinct privacy concerns of non-Western individuals. For instance, Wang et al. compared Chinese and American users' attitudes toward Online Behavioral Advertising, which involved tracking users' online behaviors and found that Chinese users were more likely to share their private data and were less concerned about potential privacy problems than Americans [65]. They guessed the reason for Chinese users' behaviors is that Chinese companies have more power to control Online Behavior Advertising than American companies [65]. Herbert et al. found that users from non-Western countries (China, India, Mexico, Saudi Arabia, and South Africa) exhibited more misconceptions about security and privacy topics than Western users, suggesting that cultural and contextual factors play a significant role in shaping privacy attitudes and behaviors. [28]. Furthermore, Fife and Orjuela compared privacy concerns between Japanese and American users and described that the concepts of "private" and "public" differed. Japanese users believed that "private" belongs to "public" [20]. Stokes et al. illustrated that using different languages to explain the same privacy policy results in different privacy concerns [57]. These concerns are shaped by a multitude of factors, encompassing cultural, linguistic, cognitive, and contextual elements. Kokolakis' exploration of the information privacy paradox further deepens this intricate web of influences. The study uncovers a common thread among individuals, transcending cultural backgrounds, wherein the allure of social rewards frequently leads them to divulge private information, causing their privacy behaviors to deviate from their stated privacy concerns [33].

Other researchers specifically investigated the Chinese privacy environment. For example, Roberts found that Chinese citizens tolerated a lack of privacy when the government obtained their personal information because the government promised specific data acquisition measures would be taken [52]. Wang and Yu interviewed Chinese users and found that they resisted giving their personal information to enterprises and the government and instead provided fake personal information to them [66].

These lines of research were primarily interested in how non-Western users were concerned about their privacy and to what extent they would choose to protect their privacy in practice. However, a significant gap was observed between users' privacy concerns and their actual privacy protection behaviors, leading to unexpected privacy risks. Given these findings, our research is motivated by the desire to understand whether similar challenges exist among Chinese internet users.

4 REVIEW OF POPULAR ONLINE PLATFORMS' PRIVACY POLICIES (STUDY 1): METHOD

After the invocation of PIPL, online platforms made changes to their operations, of which changes to their privacy polices were the most apparent. To better understand compliance with PIPL, and thus online platforms' abilities to protect the privacy of their users, we compared the privacy policies of 13 widely-used online platforms [10] before and after PIPL was invoked.

4.1 Online Platform Selection

The online platforms were selected based on the 48th Statistical Report on China's Internet Development [10]. First, we removed those online platform service types whose user utilization rate is below 70%. The remaining online platforms service types were instant messaging, online video, online payment, online shopping, search engines, and online news. Next, we selected online platforms from each online platform service type based on their rankings in the Harmony, Andriod, and IOS app stores. We then manually ranked the remaining platforms by user quantity, number of daily active users, and number of monthly active users. Finally, we chose between 1 and 4 platforms in the top 4 positions on our manually ranked list of each platform service type. The quantity we chose for each online platform service type was based on the user statistics and the percentage of users using the platform. The remaining 13 platforms included social media platforms such as WeChat ,QQ, WeiBo, and RED, video platforms like Douyin, BiliBili,, iQiyi and Kuaishou, digital payment platforms such as Alipay, shopping platforms including Taobao and Jingdong, and the Jinritoutiao platform.

4.2 Data Analysis

Firstly, this paper collected privacy policies published before and after PIPL's invocation for every online platforms. Next, this paper investigate the difference between privacy policies of same online platform to figure out how the PIPL to protect user privacy from online platforms. The difference were concluded by using keywords-in-context and text mining qualitative analyses [48] and applying measurement estimate approaches [56]. The differences between the old and new privacy policies demonstrate the efforts made by the PIPL to protect individual privacy. The new policies grant individuals the right to copy their personal information, which was not mentioned in the old version. Additionally, the new policies offer more comprehensive and detailed information regarding data processing activities compared to the previous version.

We then performed an analysis to determine how compliant privacy policies that published after PIPL's invocation were to the PIPL regulations. This data analysis was based on an open coding method [69], wherein the first author and the third author (a legal researcher), reviewed the compliance of the post-PIPL privacy polices and identified instances were the activities did not appear to be compliant. Next, the second author reviewed the activities identified by the first and third author in the privacy policies, and to compare the activities with the PIPL again to increase the accuracy of compliance of privacy policies. Then, these three authors discussed the identified activities to achieve consistency. If the three authors were not able to reach a consensus, an addition researchers was brought in and an affinity diagramming activity [26] was performed to rectify the disagreements. The privacy policies were analyzed by the first and second authors, and the accuracy of the results was reviewed by two legal researchers (the third and fourth).

5 REVIEW OF POPULAR CHINESE PLATFORMS' PRIVACY POLICIES (STUDY 1): RESULTS

Herein, we describe the changes that were found in the privacy policies of the selected online platforms after the invocation of PIPL. We also describe the non-compliant activities that was identified within the first post-PIPL privacy policies published by each online platform.

5.1 Changes to Privacy Policies Post-PIPL Invocation

Several privacy policies did improve after the invocation of PIPL (Table 1). In general, we identified three different types of changes in Post-PIPL privacy policies (Table 2): 1) the use of clearer language within privacy policies, 2) online platforms taking an expanded scope of responsibilities, and 3) additional and stronger user rights being specified.

Table 1. A comparison of platforms' privacy policies before and after PIPL's invocation. Y indicates that yes, there was a change, whereas '-' indicates that there was no change.

Items \ Companies		WeChat	QQ	Weibo	RED	Douyin	Kuaishou	iQiYi	BiliBili	Alipay	Taobao	Pinduoduo	Jingdong	Jinritoutiao
Principles	Personal Information Handling Principles	-	-	-	-	Y	-	-	-	Y	Y	Y	Y	Y
Rules	Informed Information	Y	-	-	-	-	Y	-	Y	-	Y	-	-	-
	Conditions that Waive Users' Consent -	-	-	-		Y	-	-	-	Y	Y	Y	-	Y
	Individuals' Separate Consent	Y	-	-	-	Y	-	-	-	-	Y	-	-	-
	Automated Decision-Making	Y	-	-	-	Y	Y	-	-	-	Y	-	-	-
Individuals' Rights	Right to Decide	Y	-	-	-	Y	Y	-	Y	-	-	-	-	-
	Right to Access	Y	-	-	-	-	-	-	-	-	-	-	Y	-
	Right to Copy	Y	-	-	-	Y	Y	-	-	-	-	-	-	-
	Right to Transfer	-	-	-	-	Y	Y	-	-	-	-	-	-	-
	Right to Correct	-	-	-	-	-	-	-	-	-	-	-	Y	-
	Right to Complete	-	-	-	-	-	-	-	-	-	-	-	-	-
	Right to Delete	-	-	-	-	Y	Y	-	-	-	Y	Y	Y	Y
	Right to Request Explanation	-	-	-	-	-	-	-	-	-	-	-	-	-
To Other Personal Information Handlers	Data Sharing	Y	-	-	-	Y	-	-	-	Y	Y	Y	Y	Y
	Transfer	-	-	-	-	-	-	-	-	Y	Y	Y	Y	Y
	Entrust	-	-	-	-	Y	-	-	-	Y	Y	-	-	Y

5.1.1 Utilization of Clearer Language. Online platforms made efforts to simplify and clarify their privacy policies. They reduced their use of specialized vocabulary and provided more concise rules related to information collection, handling, and sharing. In cases where simplification was not feasible, online platforms supplemented the specialized vocabulary with clearer explanations. Notably, four online platforms included a comprehensive list of their data sharing activities, encompassing the personal information processors involved, the types of information shared, the purposes of the sharing, and the methods of handling and processing the data. While some details were lacking in the provided lists, these efforts improved the transparency and user-friendliness of explaining the utilization of user data.

5.1.2 Expanded Scope of Online Platform Responsibilities. Four online platforms expanded the scope of their responsibilities detailed in their privacy policy to inform users about the online platform's responsibilities. For example, Kuaishou's updated privacy policies included provisions to notify users in the event of major changes, such as sharing users' personal information with unauthorized handlers or significant alterations to the online platform's ownership and organizational structure. Additionally, two online platforms specified reduced conditions under which individual consent could be waived, with Taobao eliminating all instances of a consent waiver. Furthermore, nearly all

Table 2. Examples of changes found in online platforms' privacy policies.

Type of Change	Before PIPL Invocation	After PIPL Invocation
Clearer Language	"We may share de-identified information with our service providers, suppliers, and other business partners. The information cannot not be associated with your identity information. Besides, the information helps us to analyze and measure the validity of the advertising and relevant services." (Jinritoutiao)	"Our business partners may need your personal information to improve their advertisement and relevant services, which includes your device information, network, advertisement clicking rate, advertisement browsing history, and advertisement display rate." (Jinritoutiao)
	"You understand and agree that, according to the law, sharing and transferring de-identified personal information, and ensuring that the data recipients cannot recover and re-identify the subject of personal information, does not belong to the sharing, transferring, and public disclosure of personal information. We do not need to inform you and obtain your consent for the storage and processing of such data." (Pinduoduo)	"You understand and agree that according to the law, anonymized personal information is not personal information. We do not need to inform you and obtain your consent for the sharing, transferring, and public disclosure of such data." (Pinduoduo)
Expanded Scope of Responsibilities	No related policies. (iQiyi)	"System permissions such as address book, location, camera, photo album (storage), microphone, calendar, etc. will not be enabled by default. The above permissions will only be accessed for specific services/functions after obtaining your separate consent." (iQiyi)
	"We will transfer your information when encountering mergers, divisions, dissolutions, declarations of bankruptcy, or other similar transactions." (Pinduoduo)	"We will transfer your information when encountering commercial cooperation, joint, merging, purchasing, asset or any similar transactions. We will provide you with the receiving company's name and contact information. Meanwhile, we will request the receivers to obey our privacy policies unless they request your consent." (Pinduoduo)
Additional and Stronger User Rights	"We will respond to your delete requisition but we cannot guarantee that we will immediately delete your personal information from our backup system." (Jingdong)	"If you successfully cancel the account, we will delete or anonymize your personal information immediately." (Jingdong)
	No related policies. (Kuaishou)	"You could check, copy, and download your personal information." (Kuaishou)

online platforms introduced regulations that required separate consent from individuals, such as Douyin's practice of obtaining separate consent when collecting facial feature information.

5.1.3 Additional and Stronger User Rights. Nine online platforms implemented significant changes to expand and enhance users' privacy rights. WeChat, for example, introduced a user portal that empowered users to manage permissions and authorizations, thus simplifying their decision-making. In addition, WeChat expanded users' access to information, such as enabling them to view their interaction history with other videos. Notably, WeChat enabled users to browse and export their personal information through a "Rights" section, thereby enhancing their ability to easily copy their data. Similarly, Douyin took steps to protect users' rights by ensuring that users refusing to authorize access to specific information only affected the use of directly related services. Douyin also introduced rules regarding the rights to copy and transfer data. While Douyin did not provide a self-export option, it guaranteed that users would be able to copy and transfer their data.

5.2 Non-Compliant Activities Specified in Privacy Policies

Several non-compliant activities were identified in the post-PIPL privacy policies and were loosely grouped into four categories (Table 3). Similar to prior work [27, 43], we also found non-compliant activities such as unclear data sharing policies, unclaimed information collecting and processing, vague data retention policies, and insufficient data protection.

5.2.1 Inadequate Risk Assessments of Sensitive Personal Information. According to PIPL, online platforms were obligated to conduct risk assessments and inform users about the risks associated with them handling users' sensitive personal information. Moreover, the law requires higher-level risk assessments and stronger safeguards for sensitive personal information compared to common information. Only four online platforms, however, demonstrated full compliance with this law, while five online platforms failed to address risk assessments in their privacy policies. Notably, QQ and WeChat, both owned by Tencent, exhibited similar privacy rules, mentioning risk assessments only in the context of providing sensitive personal information to the public. Similarly, RED mentioned risk assessments but only during data sharing activities. On the other hand, Weibo provided a

Table 3. The results of the evaluation of the online platforms' compliance with the PIPL. C indicates that the terms were compliant. P refers to "Partial", which means the corresponding privacy policies only fulfilled part of the required metrics. NM was "Not Mentioned", which means that the related terms could not be found in the privacy policies.

	WeChat	QQ	Weibo	RED	Douyin	Kuaishou	BiliBili	iQiyi	Alipay	Taobao	Pinduoduo	Jingdong	Jinritoutiao
Informed Consent	P	P	P	P	P	P	P	P	P	P	P	P	P
Waiving Consent	C	C	C	C	C	C	C	C	C	C	C	C	C
Right to Decide	C	P	C	P	P	C	C	C	P	P	P	P	C
Right to Access	C	C	C	C	C	C	C	C	C	C	C	C	C
Right to Copy	P	C	P	NM	C	C	NM	P	NM	NM	P	P	C
Right to Transfer	P	P	P	P	P	P	P	P	P	NM	P	NM	NM
Right to Correct	C	C	C	C	C	C	C	C	C	C	C	C	C
Right to Complete	C	C	C	C	C	C	C	C	C	C	C	C	C
Right to Delete	P	P	C	C	P	P	P	C	P	P	C	P	P
Right to Request Explanation	C	C	C	C	C	C	C	C	C	C	C	C	C
Disclose Personal Information	C	C	C	C	C	C	C	C	C	C	C	C	C
Processing Sensitive Personal Information	P	P	P	P	P	P	P	C	C	P	P	C	P
Automated Decision-Making	P	P	P	P	P	P	P	P	NM	P	P	P	P
Processing Minors' Personal Information	C	C	C	C	C	P	P	C	C	C	C	C	P
Rights of Close Relatives of a Deceased Natural Person	C	NM	NM	C	NM	NM	C	NM	NM	P	NM	C	NM

Table 4. The results of evaluating the compliance of platforms' terms for the right to copy. This example shows the outcomes for three online platforms. The evaluation results fell into one of four categories: Yes, No, Not Applicable, and Not Mentioned.

Metrics Evaluating the Compliance with Right to Copy	**QQ**	**Douyin**	**RED**
Does the platform provide users with the right to copy?	Yes	Yes	Not Mentioned
Can users copy their information by themselves?	Yes	No	Not Applicable
If users can exercise the right to copy by themselves, are the operations convenient (i.e., within five steps)?	Yes	Not Applicable	Not Applicable
Result	Yes	Partial	Not Mentioned

rudimentary risk assessment but lacked a more sophisticated and specific assessment for handling sensitive information.

5.2.2 Insufficient Consent Revocation Mechanisms. Among the thirteen online platforms we reviewed, three failed to provide users with a method to revoke consent and four required users to take more than five steps to revoke consent, both of which are in direct violation of Article 15 of PIPL [47]. RED, for example, did not offer any means for users to revoke their consent and Alipay required that users perform eight steps to revoke their consent.

5.2.3 Inadequate Implementation of Right to Copy and Right to Transfer. We conducted an evaluation of online platforms' compliance of the right to copy that considered three key metrics: provision of the right, a user's ability to copy their information independently, and the convenience of the copying process (Table 4).

Of the online platforms examined, four online platforms did not mention the right to copy in their privacy policies, while six did not enable users to copy their data on their own. For example, iQiYi offered users two methods to copy their data: submitting an application to the online platform or contacting consumer service. However, among the remaining three online platforms, WeChat users were required to complete a cumbersome process involving five steps to obtain their data. Furthermore, the evaluation extended to the right to transfer, revealing a similar trend, wherein the guarantees provided for the right to transfer were insufficient and mirrored the observations from the right to copy (Table 3).

5.2.4 Deficiencies in Obtaining Separate Individual Consent. A common issue that arose related to online platforms' failure to implement separate notifications and obtain separate consent from users. According to PIPL, separate consent is required in situations including the collection of sensitive information, the disclosure of personal information to third parties, and the public processing of personal information. All online platforms exhibited varying degrees of compliance, such as specifying modifications to processing purposes and sharing personal information with other information processors. For instance, Weibo's privacy regulations failed to specify that they would obtainseparate consent from individuals when commissioning other online platforms to process personal information.

It is worth noting that certain language in the privacy policies subsequent to PIPL's invocation described activities that were no longer considered to be compliant. Taobao, for example, removed the regulation "Regular disclosure of risk assessment and information handling" from its new privacy policy [47]. This resulted in it not being compliant with the regulation "The collection and processing of sensitive personal information requires prior personal information protection impact assessment and handling, and notification". Similarly, Jingdong had removed the clause "We will take all reasonable and feasible measures to ensure that no unrelated personal information is collected" from its new privacy policy [31]. The removal of this provision meant that Jingdong was no longer committed to ensuring that it collected the minimum amount of personal information, which violated the minimum data collection principle in PIPL. In addition, Jingdong deleted the clause "Security protection measures in the delivery system to prevent users' sensitive information from being exposed in the delivery process". This action signalled a decrease in Jingdong's level of protection of sensitive personal information.

5.2.5 Summary. Our findings revealed that nine online platforms made privacy policy modifications in response to PIPL and there were several significant changes, including online platforms using clearer language, taking more responsibility, and providing additional and stronger user rights. In the evaluation of the non-compliant activities described in privacy policies, four main types of non-compliance activities were found: risk assessments for sensitive personal information, insufficient consent revocation mechanisms, deficiencies in implementing the right to copy and transfer, and shortcomings in obtaining separate individual consent. Overall, the findings indicate that online platforms have responded to PIPL's requirements, however, there is still ample room for improvement before online platforms can be said to be in full compliance with PIPL.

6 UNDERSTANDING USERS' PERCEPTIONS OF PIPL (STUDY 2): METHOD

To better understand Chinese Internet users' perceptions of PIPL and their abilities to recognize non-compliant activities, semi-structured interviews were conducted with 30 interviewees. During the interviews, interviewees were also asked to perform some simple tasks, such as searching through a privacy policy to find any non-compliant activities that were specified.

6.1 Interviewees

From March to August 2022, we advertised a pre-survey on the Douban platform to recruit interviewees. In the survey, potential interviewees were asked basic questions about their demographics (i.e., age, occupation), knowledge of PIPL, and their attitudes toward PIPL. For example, we asked

"Have you heard about Personal Information Protection Law before the survey?" and *"In general, to what extent will you take measures to protect your privacy when using the platform?"*.

We received a total of 572 responses for further selection. To mitigate sample limitations, we made efforts to maximize sample diversity based on demographic information, knowledge level of PIPL, and attitudes towards privacy. Eventually, we selected 30 interviewees from various occupations, including lawyers, government staff, freelancers, unemployed individuals, policy analysis & consulting practitioners, and legal advisors. Among the interviewees, 17 were male and 13 were female (Table A1 in the Appendix A). Most interviewees had at least a college education, however, some had completed only junior education. The breakdown of interviewee responses to the pre-survey questions can be found in Table C1 in Appendix B.

6.2 Interview Procedure

Between April and August 2022, the semi-structured interviews were conducted in Mandarin Chinese using WeChat and QQ audio calls. In total, we implemented more than 30 interviews including the repeated interviews. Every interview lasted between 40 to 90 minutes via WeChat or QQ voice calls and each interviewee was paid ¥50 CNY (about $7.40 USD). All interviews were recorded with interviewees' consent.

During the interview, interviewees were asked a series of questions about their daily Internet usage, their awareness and understanding of PIPL, their perceptions about how online platforms handled their privacy and personal information, how they learned about what information online platforms collected about them and how online platforms collected such information, online platforms' consent procedures, and non-compliant activities they have observed (see Appendix B).

Then, we asked interviewees to complete two short tasks. During Task 1, interviewees were asked find the list of personal information that was collected by the online platform they mentioned in the interview and screen record themselves doing so. Then, interviewees were asked to determine if any unexpected information was mentioned in this list. Following this, we asked interviewees about their perceptions of any unexpected information they found. If this activity changed an interviewees' perceptions about privacy, we asked them any relevant semi-structured interview questions again, and we report both users' perception before and after the interview.

During Task 2, interviewees were asked to find any non-compliant terms that existed in the privacy policies from their two most frequently used platforms. For each platform, we selected two sections from the privacy policies that did not fully fulfill the requirements of PIPL and sent screenshots to interviewees on WeChat for them to read before asking them questions about the sections. For example, we displayed the information collection list from the platform's privacy policy that they used most frequently. Then we asked them, *"Do you think the app target collected information is excessive? Does the platform request your individual separate consent before collecting your information in the information list?"*.

6.3 Data Analysis

A combination of automatic transcription and manual rectification were used to transcribe the audio from the interviews. All recognizable, identifiable, and sensitive personal information in the data was removed to protect our interviewees' privacy. Then, a grounded theory approach [14, 69] was used to evaluate the interview outcomes. First, we used open coding to review the interview transcripts [69]. Two native Mandarin-speaking authors then coded the interview transcriptions separately. Then, two authors discussed the resulting codes and resolved any disagreements until reaching a mutual agreement. Next, they were attempted to find conceptual-level themes [54]. Then, the research team utilized affinity diagramming [26] to extract themes from the data, repeatedly revised them, and grouped them by sub-category [58]. Grounded theory was used to simplify and summarize the collected data and convert it into general conclusion [38].

7 UNDERSTANDING USERS' PERCEPTIONS OF PIPL (STUDY 2): RESULTS

Overall, over half of interviewees demonstrated a high level of awareness of PIPL, or at least knew the purpose and basic principles of PIPL. (Table C1) About 70 percent of interviewees thought PIPL was created to help every citizen, however, one interviewee thought that PIPL was created to help China's defense and security, as P7 described, *"When I came across this law on WeChat public account, it seemed to emphasize the procedures and regulations required for data transmission overseas".* Some interviewees also said that they thought PIPL was trying to alleviate information leakage and excessive information collection, e.g., *"I think PIPL is used to reduce information leakage and wrongdoings like spam calls. Some platforms must have revealed my phone number and identification information, which caused many spam calls. The criminals even stated my identification number precisely in the calls."* (P6).

Herein, the main findings from our study have been organized into four categories, i.e., general perceptions about privacy, the perceived effects of PIPL, non-compliant activities that were unrecognizable, and the factors influencing the imperceptibility of these activities.

7.1 General Perceptions about Privacy

The analysis uncovered several ways that public awareness, online platforms' user interfaces, and learned tolerance influenced interviewees general perceptions about privacy within China.

7.1.1 Lack of Public Awareness. Many interviewees expressed concerns about the lack of public awareness regarding personal information protection. P7 observed that privacy was not taken seriously by most Chinese individuals and that they were insensitive to issues concerning personal information. P7 further remarked that if privacy were genuinely regarded as important, the corresponding laws would have been proposed much earlier. Related to this, four interviewees mentioned that many of their acquaintances were unfamiliar with PIPL. Though some of their friends were familiar with PIPL, they did not have any ideas about how to protect their personal information and defend their rights, which reflects the current level of public awareness about privacy. P21 stated,

> *"I know that some apps definitely extracted my personal information in the background. However, as an individual, what can I do? In many cases, I just turn a blind eye to it."*

P12 expressed that he had found many reports about non-compliant activity by online platforms, however, he had never heard any news related to the outcomes of the cases, i.e., *"the government's efforts to address non-compliant activities have been inadequate and the absence of reference cases adds to our concerns".* For this interviewee, the unbalanced attention given to the entire privacy enforcement process did not instill confidence in the effectiveness of any privacy measures that were, or could be, invoked.

7.1.2 Interface Designs Prevented the Exercising of Rights. During the interviews, interviewees mentioned that platforms implemented complex user interface designs, resulting in it being challenging for them to exercise their rights, such as revoking consent. However, interviewees did not consider these complexities to be indicative of non-compliance. They understood that online platforms implemented these designs to protect their own interests, albeit at the expense of user convenience. These designs acted as a deterrent to exercise their rights because they had high transaction costs, i.e., interviewees had to search for instructions on how to revoke consent or spend additional time to click on an option to disagree. They felt that PIPL should focus on addressing issues that significantly impact their interests rather than minor inconveniences.

7.1.3 Tolerance for Non-Compliant Activities. During the interviews, interviewees expressed that protecting their personal information was an insurmountable challenge. They noted how it was hard for them as an individual to defend their rights, e.g., *"It is hard to fight with big companies. Companies have a team of top lawyers, while I might have a civilian lawyer. I don't know how I can win against the companies"* (P21).

As a result, several interviewees were accepting of certain non-compliant activities, such as app eavesdropping (e.g., when a user chats with someone in an app (or in real life) and another app recommends items mentioned in the conversation). Although P8 felt that app eavesdropping made him less comfortable, he said he could sacrifice some of his privacy for the convenience of using the app, *"it's kind of scary, but in this way (app eavesdropping) it reduces the cost of the time of searching my interested items"*. Thus, consistent with [36], there was a trade-off with more interviewees opting to compromise their privacy in favor of convenience.

Additionally, interviewees expressed concerns about privacy in the age of Big Data. P6 shared how he always had a sense of being monitored *" Once, I talked with my friend about where I planned to travel on QQ. Within ten minutes, I opened Douyin without inputting any related information and found the place that I chatted about appeared on my recommendation page"*.

7.2 Perceived Effects of PIPL

Three main themes emerged in relation to the perceived effects of PIPL on interviewees, i.e., increased transparency, the transfer of government trust to privacy concerns, and the vagueness that remains in PIPL's language.

7.2.1 Increased Transparency. The transparency of online platforms post-PIPL was a common topic. P11, who was an employee that worked on data processing at an Internet company, said that an excess of unnecessary user data was collected by online platforms pre-PIPL, but that PIPL aimed to ensure that online platforms only collected necessary data. Several interviewees also noted that post-PIPL, the list of personal information that was collected by online platforms become more visible. For example, P6 described how they became aware of PIPL through news reports that *"highlighted that certain platforms had made updates, openly displaying the data they collected from users"*. They also noted how this led them to *"explore WeChat and discover the data collection list ... it was a novel experience for me, as I felt a newfound sense of respect for my privacy."*

7.2.2 Trust in the Government Transferred to Privacy. Four interviewees did not feel as if PIPL had an effect on them, however, they still believed that their personal information privacy had improved. Interviewees expressed that over the years, the government had improved their other rights in many areas, including education, occupation, and consumption so they felt that PIPL could also improve their rights on personal information. As P2 stated, *"I personally haven't noticed any significant changes because I haven't needed to exercise my rights under PIPL yet. However, I have confidence in the government's longstanding commitment to protecting our interests, and I believe that PIPL is an important step towards safeguarding our personal information."*

7.2.3 Vagueness Inherent in PIPL's Language. Three interviewees thought that the language used within PIPL needed improvement, especially to remove concerns about vagueness in the terminology used. For example, P11 was confused about the scope of the "emergency circumstances" noted in Article 13 (4) when they were given an example of conditions of waiving consent, "There is a regulation dedicated to protecting property security, but I wonder what criteria are used to determine if a situation truly qualifies as an emergency." Similarly, P17, who was a lawyer, stated that

> *"Article 24 of PIPL provides conditions for automated decision making, but certain terms like "significantly affecting" lack clarity. While PIPL mentions that users have the right to reject automated decisions, it fails to specify an accessible process for exercising this right. Additionally, Chapter VI, which addresses the responsibilities of departments performing personal information protection duties, lacks an explicit delineation of specific obligations. This ambiguity may pose challenges for users seeking to assert their rights."*

7.3 Recognizing Non-Compliant Activities

Interviewees exhibited a range of responses with respect to the non-compliant activities that they correctly identified, incorrectly assumed were compliant, and incorrectly assumed were non-compliant.

7.3.1 True Positive Non-Compliant Activities. Several factors were found to help interviewees recognize non-compliant activities, such as having a legal knowledge background, legal regulations being provided for reference, and interviewees' previous experiences with the terminology used in privacy policies. For those without a legal background, attention-grabbing text and visuals were helpful when determining non-compliant activities. For example, when a bold font style was used to highlight sensitive information, interviewees easily focused on it and were able to identify the excessive collection of personal information.

Interviewees correctly believed that app eavesdropping was a non-compliant and illegal activity since they thought that online platforms failed to ask them for permission to do so. Some interviewees thought that some data was collected without their permission, like device information, however, most interviewees were unbothered by this as the collection of such non-sensitive data would not influence their lives, e.g., *"I hate platforms collecting my data without my permission but it doesn't matter because the leak of device information will be no impact on my life"* (P3).

7.3.2 False Negative Non-Compliant Activities. During the interviews, we found that interviewees incorrectly identified some activities as being compliant, for example, waiving consent. Surprisingly, we found that although interviewees believed their consent should be always obtained if online platforms collected and handled their information, sixteen interviewees thought that the government could collect and handle their personal information without their consent.

Two interviewees mentioned that Chinese people generally received a patriotic education, which emphasized collectivism at a young age. P28 described that Chinese people tended to transfer their love for country into trust in government since almost no one distinguished "country" and "government" in China, i.e., *"We've always been taught to be patriotic. Meanwhile, no one tells us the differences between the state and the government. Many people feel that the state equals the government and the trust in government somehow stems from the patriotism we have been taught."*

Some interviewees thus held altruistic beliefs and were willing to "sacrifice" their personal information to contribute to society. For example, P12 felt that his personal information was a way to help the government learn about more diverse conditions and make wiser decisions, i.e., *"After all, I represent part of the public opinions. I feel that I am willing to cede control of my personal information to the government if it benefits more people. I hope my information can let the government know the needs of more people."* Although the government had stored a lot of personal information and could do harmful things with it, P2 stated that "If the government wanted to do something against you, the government would have done so long ago."

7.3.3 False Positive Non-Compliant Activities. Interviewees missed identifying several online platform activities that were non-compliant. For example, interviewees identified the inconvenience of revoking consent via the multiple pop-ups within online platforms that were used to obtain personal consent, however, they did not believe that being inconvenienced was a non-compliant activity. Instead, they regarded this non-compliant activity as simply a challenge for further improvement. Three interviewees, regarded these practises as “rogue" and believed that online platforms utilized them to legitimize their “harassment” of users, e.g., *“I did not give the food delivery app permission to use the camera , but the app asked me for the permission three times in a day”* (P24).

As iOS devices have the option to ask an application not to track a user, some interviewees thought this option was a by-product of online platforms trying to meet the requirements of PIPL. Therefore, they thought that if they chose this option, platforms would not collect their data and their search records would not appear in search engines, e.g., *“I changed my phone in January this year and I needed to download all the new software. I found a lot of pop-ups asking me to ask for no tracking at that time, however, I think there was nothing changed. In theory, if I chose ‘No Tracking’, I would not have my search shopping history inside Taobao”* (P1). This uncertainty surrounding the practical impact of such privacy options on online platforms underscores the need for more transparent information and education for users regarding the actual outcomes of their choices.

Interviewees’ abilities to recognize, for example, missing details about third-party online platforms’ contact information depended on the interviewees’ level of knowledge. For example, P5, who was concerned about third-party data sharing, exhibited no hesitation in pointing out the cases where insufficient third-party information was provided and also listed the missing information, whereas several other interviewees who were not concerned about this did not identify this missing data. In general, the limited knowledge and awareness of individuals, combined with a generally high tolerance for non-compliant practices, hindered interviewees abilities to recognize non-compliant activities.

In addition, the presentation design of privacy policies was also found to further complicate the identification of non-compliant activities. During Task 2, interviewees received an expert of a privacy policy and reviewed large screenshots with sparse text in them, which is more favorable than viewing a privacy policy on a small mobile phone screen as they would do in their daily life. All interviewees thus complained about the intolerable length of traditional privacy policies. They also noted that the use of bold fonts was often not obvious and that this led them to skip some core parts of privacy policies. Some interviewees also thought that some online platforms even bolded the wrong text to mislead users and prevent them from reading important terms, e.g., *“In one article, the "real-name system" and the relevant law were highlighted, indicating their importance. However, the same article mentioned the sharing of identity card information with other applications owned by the same company, which I found unsuitable. Surprisingly, this particular information was not highlighted or given similar emphasis.”* (P28).

8 DISCUSSION

The two studies that were conducted identified the changes and implications of the invocation of China’s PIPL. This research is not only one of the first systematic investigations of PIPL, but also contributes to the burgeoning attention that is being devoted to the legal regulation of privacy and personal information and illuminates the troublesome practices and perceptions of personal information protection that exist. Beyond this, our findings add to the scarce literature on non-Western users’ privacy concerns, which can greatly advance the scholarly understanding of the influence of cultural differences on the awareness of privacy protection and public-private boundaries.

Previous research has extensively examined the compliance landscape of applications under GDPR and identified common privacy concerns, including complex permission revocation procedures, obscure privacy language, and inadequate data handling. Building upon this body of work, our study explores similar issues prevalent in online platforms within the Chinese context, including inadequate consent revocation mechanisms, deficiencies in implementing the right to copy and transfer data, and shortcomings in obtaining separate individual consent [5, 18, 34]. While some common privacy concerns align with prior studies, our research also identified unique challenges specific to Chinese platforms, such as the lack of risk assessment and user notification, calling for tailored approaches to enhance privacy protection.

Our study aligns with the previous studies [52, 65], emphasizing the presence of a lack of privacy awareness and conceptual understanding within the Chinese context. In line with the findings from Wang et al. [65], our research affirms that Chinese users tend to be willing to share their private data and exhibit lower concerns about potential privacy issues. This highlights a higher degree of insensitivity towards privacy among Chinese users, leading to a greater acceptance of non-compliant activities. Furthermore, in scenarios involving the tracking of users' online behaviors, Chinese users display a sophisticated understanding of automated algorithms. Building upon the findings by Wang et al. [65], our research reveals that this extensive comprehension often results in users prioritizing convenience over personal privacy.

In the study conducted by Fife and Orjuela [20], it was emphasized that Japanese users perceive "private" as falling within the "public" domain, whereas Chinese internet users hold a contrasting perspective, where "private" is distinct from the "public" domain. This divergence in outlook can be attributed to variations in their trust in the government and their altruistic beliefs. The level of trust individuals have in the government significantly influences their perceptions of privacy and their readiness to disclose personal information. This underscores the crucial need to account for societal attitudes and cultural factors when formulating privacy policies in non-Western contexts. In our research, more than half of the participants expressed a willingness to share their information with the government or make it public. However, for some users, this willingness was tinged with reluctance, as they felt powerless as individuals within the broader societal context. Nevertheless, it is crucial to recognize that these privacy behaviors may not be consistent across all Chinese users, and there can be variations in their levels of trust and willingness to share information. People's attitudes are intricate and multifaceted, shaped by factors beyond nationality, encompassing elements such as ethnicity, religion, socioeconomic status, and personal experiences.

Based on these findings, there are several implications for the three stakeholders engaged in personal information protection, i.e., lawmakers, personal information processors (i.e., online platforms), and users.

8.1 Implications

8.1.1 Implications for Lawmakers. Our results demonstrated that PIPL still requires refinement to maximize its effectiveness. Consequently, for lawmakers, our findings provide timely and detailed feedback on the current state of PIPL execution, which can assist legal authorities in assessing the design and implementation of PIPL. In particular, by making references to information about the non-compliant activities found in the privacy policies of the thirteen online platforms, lawmakers can clarify the regulations and strengthen the enforcement of the corresponding activit ies in a targeted way, for example, the clarification of the scope of *"other personal information processing activities that have a significant impact on individual rights"* (Article 55 [47]).

Additionally, as interviewees emphasized the importance of flexibility and adaptability in the development of legislation, we recommend that lawmakers conduct regular user interviews and assessments of online platform compliance (similar to our study), to determine whether online platforms are properly protecting users' privacy. Furthermore, we suggest that lawmakers engage in more extensive research to identify areas of the PIPL that may require adjustments or strengthening, such as emerging issues with technologies such as artificial intelligence, biometric identification, and Internet of Things devices. By doing so, lawmakers can ensure that the PIPL is a more effective privacy standard.

Likewise, considering the confusion caused by the inconsistent and potentially misleading use of bold font styles, we strongly advise lawmakers to take proactive measures in creating standardized guidelines for regulating the interface design of application privacy policies. These guidelines should cover the proper usage of font styles, such as when to employ bold, italic, underline, and when to utilize uppercase or lowercase letters. The overarching goal is to mitigate user confusion and improve clarity in privacy policy presentation.

In the cultural context of China, privacy remains a relatively nascent concept. It is noteworthy that many Chinese individuals lack an understanding of privacy, which lead to an insufficient emphasis being placed upon its importance [65]. In line with this, our study also found limitations in interviewees' comprehension of PIPL and the concept of informed consent. It is thus imperative for government authorities to increase the public's legal education to raise the public's awareness of privacy protection and rectify misunderstandings about PIPL and its goals.

8.1.2 Implications for Personal Information Processors. Our study highlighted the need for personal information processors, i.e., online platforms, to engage in more rigorous and active implementations of PIPL and for them to develop more user-friendly privacy services to facilitate user rights protection.

It was not uncommon to find non-compliant activities within post-PIPL privacy policies (Table 3). Therefore, personal information processors should conduct self-assessments about the degree to which they fulfill PIPL and correct non-compliant activities that are part of their operations. For instance, personal information processors need to ensure proper user consent is obtained and conduct risk assessments before sharing users' data with other processors. Furthermore, personal information processors should consider implementing user interface designs that alleviate user privacy concerns and make it easy to revoke consent. Additionally, to address concerns about background data collection, online platforms should provide users with a daily summary of collected information, specifying the data collected throughout the day and its specific purposes.

Considering that users often have limited legal knowledge and reading through privacy policies places a great burden on them, personal information processors should make efforts to improve privacy policy transparency, conciseness, and clarity. One approach could be to design more user-friendly interfaces that present privacy terms in a succinct, readable ways. Such designs should accurately highlight the most salient aspects of the privacy policy and possibly incorporate visual elements, where appropriate. For example, personal information processors could create informative videos that provide clear explanations of their data collection and usage practices, as well as inform users about their rights, similar to those found in Google's [23], Facebook's [42], and the Guardian's privacy policies [25]. This practise would improve user understanding and engagement with privacy materials and matters.

Collaboration between personal information processors and authoritative legal institutions would also be a valuable approach to alleviate the burdens currently placed on users to safeguard their rights. For example, legal institutions could compile a risk advisory table for privacy policies. The table could highlight potential non-compliant provisions and serve as a useful resource to alert users about potential risks. Furthermore, when all provisions in a privacy policy are compliant with the applicable regulations and standards, a legal certification could be granted, assuring users that the personal information processor had adhered to necessary privacy practices and requirements.

8.1.3 Implications for Users. Users, who are the intended beneficiaries of PIPL, also have a crucial role to play in promoting personal information protection. It became evident from interviewees' misunderstandings about the right of informed consent that there is a need to enhance the public's awareness of personal information and users' abilities to safeguard personal information effectively. In light of this result, users should prioritize staying up to date on the latest privacy regulations and best practices related to personal information protection. While it is true that privacy policies can be dense and challenging to navigate, there are several steps users can take to overcome this hurdle. One approach is to seek information from reputable sources that provide simplified explanations and summaries of privacy policies. Additionally, users can actively engage in educational initiatives and workshops that focus on privacy rights and practices. These initiatives can help users better understand the implications of sharing personal information and how to make informed choices when interacting with online platforms.

Furthermore, users should exercise caution when sharing personal information, particularly on social media platforms. While being mindful of the potential risks, users should evaluate the necessity and appropriateness of sharing sensitive details and avoid disclosing sensitive information unless absolutely necessary. In addition, users should pay more attention to the issue of personal information leakage in their everyday use of online platforms. For example, users need to be aware of the permissions they grant to online platforms and regularly review their privacy settings within social media accounts, applications, and other online platforms. By actively managing privacy settings, users can maintain better control over their personal information. Lastly, we recommend that users take proactive steps to build up necessary knowledge and skills in rights protection. Users should educate themselves about privacy rights, understand how to exercise control over their personal data, and become aware of the actions they can take to protect their privacy.

By following these suggestions, users can contribute to the promotion of personal information protection and play an active role in safeguarding their own privacy rights.

8.2 Limitations

While we attempted to recruit a diverse interviewee pool and sample a range of online platform privacy policies, this research does, however, have several limitations. First, the survey respondents and interviewees in our study were only recruited through the Douban platform, which may skew the sample toward active users of Douban. Though the gender, age, and educational level distribution of the sample was reasonably balanced, it was still limited in its representativeness of Chinese Internet users. In the future, a more inclusive recruitment strategy should be used to strengthen the diversity of the selected sample. Additionally, this research mainly examined Chinese Internet users' perceptions of PIPL and the right of informed consent. Given that the implementation of PIPL is an ongoing process, privacy policies constantly change, and users' mindsets and perceptions evolve over time, future longitudinal research is needed to monitor any changes that occur and track long-term trends that emerge.

9 CONCLUSION

This research used a two-pronged approach to understand the effects of invoking PIPL in China on users and online platforms. In Study 1, a review of the privacy policies of 13 prominent platforms was conducted to identify any changes that occurred post-PIPL invocation. The findings revealed that the privacy policies generally became more user-friendly and employed simpler language and logical structures. Platforms also demonstrated an increased obligation to inform users and provide stronger individual rights protection. During the evaluation, we identified four instances of non-compliant activities, including not having a prior personal information risk assessment when handling sensitive data and the failure to obtain separate consent from users.

In Study 2, we examined the perceptions of 30 Chinese Internet users regarding PIPL. Interviewees exhibited a high level of awareness regarding PIPL, with a basic understanding of its purpose and fundamental principles. Furthermore, we identified factors that influenced interviewees' attitudes towards PIPL, including the interface designs that were used and the vague language contained within PIPL. We also evaluated interviewees' ability to recognize non-compliant activities, finding that while interviewees were generally able to identify obvious non-compliant activities such as app eavesdropping and excessive data collection, they struggled with recognizing activities related to obtaining separate consent. Interviewees' difficulties in identifying non-compliant activities were attributed to factors such as their trust in the government, which lead to them having a higher tolerance for non-compliant behaviors.

Lawmakers, personal information processors, users, and future researchers should be able to draw on our findings and implications to improve personal information practices in China and potentially worldwide.

REFERENCES

[1] Mamtaj Akter, Leena Alghamdi, Dylan Gillespie, Nazmus Sakib Miazi, Jess Kropczynski, Heather Lipford, and Pamela J Wisniewski. 2022. CO-oPS: A Mobile App for Community Oversight of Privacy and Security. In *Companion Publication of the 2022 Conference on Computer Supported Cooperative Work and Social Computing*. 179–183. https://doi.org/10.1145/3500868.3559706

[2] Darcy WE Allen, Alastair Berg, Chris Berg, Brendan Markey-Towler, and Jason Potts. 2019. Some economic consequences of the GDPR. *Allen DWE, Berg A, Berg C, Markey-Towler B and Potts J (2019)'Some Economic Consequences of the GDPR', Economics Bulletin* 39, 2 (2019), 785–797.

[3] Markus Andresen, Martin Bjerke, Thorben Dahl, Aksel Langø Karlsen, Brage Staven, and Erik Wiker. [n. d.]. The General Data Protection Regulation-Affecting User Perception of IoT Related Privacy Concerns? ([n. d.]).

[4] David Basin, Søren Debois, and Thomas Hildebrandt. 2018. On purpose and by necessity: compliance under the GDPR. In *International Conference on Financial Cryptography and Data Security*. Springer, 20–37. https://doi.org/10.1007/978-3-662-58387-6_2

[5] Alex Bowyer, Jack Holt, Josephine Go Jefferies, Rob Wilson, David Kirk, and Jan David Smeddinck. 2022. Human-GDPR Interaction: Practical Experiences of Accessing Personal Data. In *CHI Conference on Human Factors in Computing Systems*. 1–19. https://doi.org/10.1145/3491102.3501947

[6] Martin Brodin. 2019. A framework for GDPR compliance for small-and medium-sized enterprises. *European Journal for Security Research* 4, 2 (2019), 243–264. https://doi.org/10.1109/ISSRE5003.2020.00032

[7] Igor Calzada. 2022. Citizens' data privacy in China: The state of the art of the Personal Information Protection Law (PIPL). *Smart Cities* 5, 3 (2022), 1129–1150. https://doi.org/10.3390/smartcities5030057

[8] Lelio Campanile, Mauro Iacono, Fiammetta Marulli, and Michele Mastroianni. 2021. Designing a GDPR compliant blockchain-based IoV distributed information tracking system. *Information Processing & Management* 58, 3 (2021), 102511. https://doi.org/10.1016/j.ipm.2021.102511

[9] C Castelluccia, S Guerses, M Hansen, JH Hoepman, J van Hoboken, B Vieira, et al. 2017. Privacy and data protection in mobile applications: A study on the app development ecosystem and the technical implementation of GDPR. (2017). https://doi.org/10.2824/114584

[10] China Internet Network Information Center. 2021. The 48th Statistical Report on China's Internet Development (in Chinese). (September 2021).

[11] Xiao Cheng. 2021. Analyzing General Provisions of Personal Information Protection Law of the People's Republic of China (in Chinese). *Journal of National Prosecutors College* 29, 5 (2021), 3–20.

[12] Xiao Cheng. 2021. Analyzing Personal Information Handling Rules of Personal Information Protection Law of the People's Republic of China (in Chinese). *Tsinghua University Law Journal* 3 (2021).

[13] European Union Commission. 2016. General Data Protection Law. https://gdpr-info.eu/, Accessed August 2nd, 2022.

[14] Juliet Corbin and Anselm Strauss. [n. d.]. Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory. Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory, 2012.

[15] People's Daily. 2021. Concerned about the protection of personal information: why do cell phones "know" me so well? (in Chinese). https://www.chinanews.com.cn/gn/2021/11-01/9599189.shtml, Accessed July 27, 2022.

[16] Southern Metropolis Daily·Wancaishe. 2022. What is the status quo of App supervision after the implementation of the Personal Insurance Law? What changes have occurred in the enterprise? Experts discuss (in Chinese). https://finance.eastmoney.com/a/202212252597298690.html, Accessed Jan 9th, 2023.

[17] Ming Fan, Le Yu, Sen Chen, Hao Zhou, Xiapu Luo, Shuyue Li, Yang Liu, Jun Liu, and Ting Liu. 2020. An Empirical Evaluation of GDPR Compliance Violations in Android mHealth Apps. In *2020 IEEE 31st International Symposium on Software Reliability Engineering (ISSRE)*. 253–264. https://doi.org/10.1109/ISSRE5003.2020.00032

[18] Ming Fan, Le Yu, Sen Chen, Hao Zhou, Xiapu Luo, Shuyue Li, Yang Liu, Jun Liu, and Ting Liu. 2020. An empirical evaluation of GDPR compliance violations in Android mHealth apps. In *2020 IEEE 31st international symposium on software reliability engineering (ISSRE)*. IEEE, 253–264. https://doi.org/10.1109/ISSRE5003.2020.00032

[19] Casey Fiesler, Michaelanne Dye, Jessica L Feuston, Chaya Hiruncharoenvate, Clayton J Hutto, Shannon Morrison, Parisa Khanipour Roshan, Umashanthi Pavalanathan, Amy S Bruckman, Munmun De Choudhury, et al. 2017. What (or who) is public? Privacy settings and social media content sharing. In *Proceedings of the 2017 ACM conference on computer supported cooperative work and social computing*. 567–580. https://doi.org/10.1145/2998181.2998223

[20] Elizabeth Fife and Juan Orjuela. 2012. The privacy calculus: Mobile apps and user perceptions of privacy and security. *International Journal of Engineering Business Management* 4, Godište 2012 (2012), 4–11. https://doi.org/10.5772/51645

[21] Mélanie Bourassa Forcier, Hortense Gallois, Siobhan Mullan, and Yann Joly. 2019. Integrating artificial intelligence into health care through data access: can the GDPR act as a beacon for policymakers? *Journal of Law and the Biosciences* 6, 1 (2019), 317. https://doi.org/10.1093/jlb/lsz013

[22] Felipe González, Andrea Figueroa, Claudia López, and Cecilia Aragon. 2019. Information Privacy Opinions on Twitter: A Cross-Language Study. In *Conference Companion Publication of the 2019 on Computer Supported Cooperative Work and Social Computing*. 190–194. https://doi.org/10.1145/3311957.3359501

[23] Google. 2023. Google Privacy Policy. https://policies.google.com/privacy?hl=en-US/, Accessed July 13, 2023.

[24] Jie Gu, Yunjie Calvin Xu, Heng Xu, Cheng Zhang, and Hong Ling. 2017. Privacy concerns for mobile app download: An elaboration likelihood model perspective. *Decision Support Systems* 94 (2017), 19–28. https://doi.org/10.1016/j.dss.2016.10.002

[25] The Guardian. 2019. The Guardian's Privacy Policy. https://www.theguardian.com/info/video/2019/sep/12/the-guardians-privacy-policy-video, Accessed July 13, 2023.

[26] Rex Hartson and Pardha Pyla. 2012. *The UX Book: Process and Guidelines for Ensuring a Quality User Experience* (1st ed.). Morgan Kaufmann Publishers Inc., San Francisco, CA, USA.

[27] Saad Sajid Hashmi, Nazar Waheed, Gioacchino Tangari, Muhammad Ikram, and Stephen Smith. 2021. Longitudinal compliance analysis of android applications with privacy policies. In *International Conference on Mobile and Ubiquitous Systems: Computing, Networking, and Services*. Springer, 280–305. https://doi.org/10.1007/978-3-030-94822-1_16

[28] Franziska Herbert, Steffen Becker, Leonie Schaewitz, Jonas Hielscher, Marvin Kowalewski, Angela Sasse, Yasemin Acar, and Markus Dürmuth. 2023. A World Full of Privacy and Security (Mis) conceptions? Findings of a Representative Survey in 12 Countries. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*. 1–23. https://doi.org/10.1145/3544548.3581410

[29] Supervision in China. 2021. The era of brutal gold mining for personal information is over (in Chinese). http://www.npc.gov.cn/npc/c30834/202111/06172ca5e0ff4fde800d19d734b63206.shtml, Accessed July 27, 2022.

[30] Steven J Jackson, Tarleton Gillespie, and Sandy Payette. 2014. The policy knot: Re-integrating policy, practice and design in CSCW studies of social computing. In *Proceedings of the 17th ACM conference on Computer supported cooperative work & social computing*. 588–602. https://doi.org/10.1145/2531602.2531674

[31] Jingdong. 2021. Privacy Policy of Jingdong (in Chinese). https://hlc.m.jd.com/privacy/, Accessed January 1, 2021.

[32] Smirity Kaushik, Yaxing Yao, Pierre Dewitte, and Yang Wang. 2021. "How I Know For Sure": People's Perspectives on Solely Automated Decision-Making (SADM). In *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*. USENIX Association, 159–180. https://www.usenix.org/conference/soups2021/presentation/kaushik

[33] Spyros Kokolakis. 2017. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & security* 64 (2017), 122–134.

[34] Lin Kyi, Sushil Ammanaghatta Shivakumar, Cristiana Teixeira Santos, Franziska Roesner, Frederike Zufall, and Asia J Biega. 2023. Investigating deceptive design in GDPR's legitimate interest. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*. 1–16. https://doi.org/10.1145/3544548.3580637

[35] Xabier Larrucea, Micha Moffie, Sigal Asaf, and Izaskun Santamaria. 2020. Towards a GDPR compliant way to secure European cross border Healthcare Industry 4.0. *Computer Standards & Interfaces* 69 (2020), 103408. https://doi.org/10.1016/j.csi.2019.103408

[36] Josephine Lau, Benjamin Zimmerman, and Florian Schaub. 2018. Alexa, are you listening? Privacy perceptions, concerns and privacy-seeking behaviors with smart speakers. *Proceedings of the ACM on human-computer interaction* 2, CSCW (2018), 1–31.

[37] Claire Laybats and John Davies. 2018. GDPR: Implementing the regulations. *Business Information Review* 35, 2 (2018), 81–83. https://doi.org/10.1177/0266382118777808

[38] Michael Lewis-Beck, Alan E Bryman, and Tim Futing Liao. 2003. *The Sage encyclopedia of social science research methods*. Sage Publications.

[39] Thomas Linden, Rishabh Khandelwal, Hamza Harkous, and Kassem Fawaz. 2018. The privacy policy landscape after the GDPR. *arXiv preprint arXiv:1809.08396* (2018). https://doi.org/10.48550/arXiv.1809.08396

[40] Peder Lind Mangset. 2018. *Analysis of mobile application's compliance with the general data protection regulation (gdpr).* Master's thesis. NTNU. http://hdl.handle.net/11250/2560789

[41] Davit Marikyan, Savvas Papagiannidis, Rajiv Ranjan, and Omer Rana. 2021. *General Data Protection Regulation: An Individual's Perspective.* Association for Computing Machinery, New York, NY, USA. https://doi.org/10.1145/3492323.3495620

[42] Meta. 2023. Meta Privacy Policy. https://www.facebook.com/privacy/policy/, Accessed July 13, 2023.

[43] Jayashree Mohan, Melissa Wasserman, and Vijay Chidambaram. 2019. Analyzing GDPR compliance through the lens of privacy policy. In *Heterogeneous Data Management, Polystores, and Analytics for Healthcare*. Springer, 82–95. https://doi.org/10.1007/978-3-030-33752-0_6

[44] Susan Mok. 2021. The PRC Personal Information Protection Law and its Regulatory Impact on Multinational Entities. *China Law & Practice* (Sep 24 2021). https://lbapp01.lib.cityu.edu.hk/ezlogin/index.aspx Copyright - Copyright ALM Media Properties, LLC Sep 24, 2021; Last updated - 2021-09-24; SubjectsTermNotLitGenreText - China.

[45] Business observation website. 2022. "Personal Information Security Annual Report (2022)" is released: App personal information protection level has been significantly improved (in Chinese). http://news.hexun.com/2022-12-30/207571508.html, Accessed Jan 9th, 2023.

[46] Cyberspace Administration of China. 2022. Decision of the Cyberspace Administration of China to make administrative punishment related to network security review in accordance with the law for DDT Global Co (in Chinese). https://mp.weixin.qq.com/s/6v-BVICScq1loDmdx7x9ww, Accessed July 30, 2022.

[47] The Nation People's Congress of the People's Republic of China. 2021. Personal Information Protection Law of the People's Republic of China (in Chinese). (2021). http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml

[48] Anthony J Onwuegbuzie, Nancy L Leech, and Kathleen MT Collins. 2012. Qualitative analysis techniques for the review of the literature. *Qualitative Report* 17 (2012), 56.

[49] Chinju Paul, Kevin Scheibe, and Sree Nilakanta. 2020. Privacy concerns regarding wearable IoT devices: how it is influenced by GDPR?. In *Proceedings of the 53rd Hawaii International Conference on System Sciences*.

[50] Annika Pinch, Jeremy Birnholtz, Ashley Kraus, Kathryn Macapagal, and David A. Moskowitz. 2021. "It's not exactly prominent or direct, but it's there": Understanding Strategies for Sensitive Disclosure Online. In *Companion Publication of the 2021 Conference on Computer Supported Cooperative Work and Social Computing*. 149–152. https://doi.org/10.1145/3462204.3481740

[51] Wanda Presthus and Hanne Sørum. 2018. Are consumers concerned about privacy? An online survey emphasizing the general data protection regulation. *Procedia Computer Science* 138 (2018), 603–611. https://doi.org/10.1016/j.procs.2018.10.081

[52] Huw Roberts. 2021. Informational Privacy with Chinese Characteristics. *Digital Ethics Lab Yearbook* (2021).

[53] Nader Sohrabi Safa, Faye Mitchell, Carsten Maple, Muhammad Ajmal Azad, and Mohammad Dabbagh. 2022. Privacy Enhancing Technologies (PETs) for connected vehicles in smart cities. *Transactions on Emerging Telecommunications Technologies* 33, 10 (2022), e4173. https://doi.org/10.1002/ett.4173

[54] Maggi Savin-Baden and Claire Howell Major. 2023. *Qualitative research: The essential guide to theory and practice.* Taylor & Francis.

[55] Jannick Sørensen and Sokol Kosta. 2019. Before and after gdpr: The changes in third party presence at public and private european websites. In *The World Wide Web Conference*. 1590–1600. https://doi.org/10.1145/3308558.3313524

[56] Steven E Stemler. 2004. A comparison of consensus, consistency, and measurement approaches to estimating interrater reliability. *Practical Assessment, Research, and Evaluation* 9, 1 (2004), 4. https://doi.org/10.7275/96jp-xz07

[57] Jackson Stokes, Tal August, Robert A Marver, Alexei Czeskis, Franziska Roesner, Tadayoshi Kohno, and Katharina Reinecke. 2023. How language formality in security and privacy interfaces impacts intended compliance. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*. 1–12. https://doi.org/10.1145/3544548.3581275

[58] A. Strauss and J.M. Corbin. 1997. *Grounded Theory in Practice.* SAGE Publications. https://books.google.com.hk/books?id=TtRMolAapBYC

[59] Joanna Strycharz, Jef Ausloos, and Natali Helberger. 2020. Data protection or data frustration? Individual perceptions and attitudes towards the GDPR. *Eur. Data Prot. L. Rev.* 6 (2020), 407. https://doi.org/1021552/edpl/2020/3/10

[60] Sun and Shadow Flying Fun 51. 2020. How can we protect personal information when mobile apps are overly invasive of privacy? (in Chinese). https://www.freebuf.com/articles/database/239684.html, Accessed July 29, 2022.

[61] Radek Tahal and Tomáš Formánek. 2020. Reflection of GDPR by the Czech Population. *Management & Marketing* 15, 1 (2020), 78–94. https://doi.org/10.2478/mmcks-2020-0005

[62] Nguyen Binh Truong, Kai Sun, Gyu Myoung Lee, and Yike Guo. 2019. Gdpr-compliant personal data management: A blockchain-based solution. *IEEE Transactions on Information Forensics and Security* 15 (2019), 1746–1761. https:

//doi.org/10.1109/TIFS.2019.2948287

[63] Christine Utz, Martin Degeling, Sascha Fahl, Florian Schaub, and Thorsten Holz. 2019. (Un) informed consent: Studying GDPR consent notices in the field. In *Proceedings of the 2019 acm sigsac conference on computer and communications security*. 973–990. https://doi.org/10.1145/3319535.3354212

[64] Iris Van Ooijen and Helena U Vrabec. 2019. Does the GDPR enhance consumers' control over personal data? An analysis from a behavioural perspective. *Journal of consumer policy* 42, 1 (2019), 91–107. https://doi.org/10.1007/s10603-018-9399-7

[65] Yang Wang, Huichuan Xia, and Yun Huang. 2016. Examining American and Chinese internet users' contextual privacy preferences of behavioral advertising. In *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing*. 539–552. https://doi.org/10.1145/2818048.2819941

[66] Zhong Wang and Qian Yu. 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 (2015), 782–792. https://doi.org/10.1016/j.clsr.2015.08.006

[67] Christian Wirth and Michael Kolain. 2018. Privacy by blockchain design: a blockchain-enabled GDPR-compliant approach for handling personal data. In *Proceedings of 1st ERCIM Blockchain Workshop 2018*. European Society for Socially Embedded Technologies (EUSSET). https://doi.org/10.18420/blockchain2018_03

[68] Richmond Y Wong, Andrew Chong, and R Cooper Aspegren. 2023. Privacy Legislation as Business Risks: How GDPR and CCPA are Represented in Technology Companies' Investment Risk Disclosures. *Proceedings of the ACM on Human-Computer Interaction* 7, CSCW1 (2023), 1–26. https://doi.org/10.1145/3579515

[69] Brad Wuetherick. 2010. Review: "Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory 3e" (Corbin and Strauss). 36 (12 2010). https://doi.org/10.21225/D5G01T

[70] Chen Xuan-bo. 2020. Personal Information Protection and Improvement of Information Disclosure System for Network Service Providers (in Chinese). *Journal of South-Central Minzu University (Humanities and Social Sciences)* 40, 1 (2020), 174–180.

APPENDIX A - INTERVIEWEE DEMOGRAPHICS

Table A1. Summary of the Chinese Internet users interviewed. Among the 30 interviewees, 15 were female and 15 were male. They were between 18 and 60 years of age. Twenty-four had a Bachelor's Degrees or higher. It is worth noting that 6 interviewees were government staff, 4 were legal practitioners, and 1 was a professor.

Interviewee ID	Gender	Age	Education Level	Occupation
P1	Female	18-20	Bachelor's Degree	Student
P2	Female	41-45	Bachelor's Degree	Government Staff
P3	Male	21-25	Bachelor's Degree	Technical Director of a Construction company
P4	Female	26-30	Associate Degree	Government Staff
P5	Female	26-30	Master's Degree or Higher	Teacher
P6	Male	18-20	Bachelor's Degree	Student
P7	Female	18-20	Bachelor's Degree	Student
P8	Male	18-20	Bachelor's Degree	Student
P9	Male	18-20	Bachelor's Degree	Student
P10	Male	21-25	Bachelor's Degree	Preferred not to say
P11	Female	21-25	Bachelor's Degree	Employed at an Internet Company
P12	Male	31-35	Master's Degree or Higher	Government Staff
P13	Female	36-40	Bachelor's Degree	Government Staff
P14	Male	21-25	Associate Degree	Policy Analysis & Consulting Practitioner
P15	Male	26-30	Master's Degree or Higher	Lawyer
P16	Female	26-30	Master's Degree or Higher	Product Manager at an Internet company
P17	Female	26-30	Bachelor's Degree	Lawyer
P18	Male	31-35	Master's Degree or Higher	Professor
P19	Male	26-30	Master's Degree or Higher	Urban Planner
P20	Female	36-40	Bachelor's Degree	Legal Advisor
P21	Female	31-35	Master's Degree or Higher	Human Resources Administrator for an Internet company
P22	Male	46-50	Junior High or Lower	Freelancer
P23	Male	36-40	Bachelor's Degree	IT Marketer
P24	Female	46-50	Associate Degree	Retiree
P25	Female	41-45	Associate Degree	Freelancer
P26	Female	36-40	Master's Degree or Higher	Salesperson
P27	Female	31-35	Bachelor's Degree	Freelance Journalist
P28	Male	56-60	Bachelor's Degree	Government Staff
P29	Male	45-50	Bachelor's Degree	Government Staff
P30	Male	41-45	Senior High	Unemployed

APPENDIX B - INTERVIEW QUESTIONS

(1) What is your occupation?
(2) How often do you use online video/social/online shopping mobile applications?
(3) To what extent do you protect your personal information during daily life?
(4) (If the interviewee said "I have heard about the PIPL" in the pre-survey) Have you heard about the personal information protection law?
  (a) How did you learn about PIPL?
  (b) What is the effect of the PIPL? Who is PIPL designed for?

    (c) What do you think of PIPL?
        (i) Why do (not) you want to learn about the PIPL?
        (ii) In the pre-survey, you said that "the personal information protection law (does not) strengthen the right you have". What is the reason?

(5) What is informed consent?
(6) Have you executed the right to know?
(7) If you knew the right to know before, how do you want to use this right?
(8) How do you think the progress of the application you used most frequently in informed consent?
(9) After the implementation of PIPL, did you perceive a change of informed consent in your most frequently used application? If yes, please describe it.
(10) Do you feel that you have learned more about informed consent than before the implementation of PIPL? If yes, Please describe it.
(11) Do you feel that your power to control your personal information is stronger than before the implementation of PIPL? If yes, please describe it. In what aspects do you feel the change?
(12) What personal information did you know was collected by the application you used?
(13) What do you know about personal information collection cases?
(14) What notification does the application give to you while the application is collecting the above personal information? Please give us some detailed examples.
    (a) What information do you think the application still should tell except the above?
(15) Is there any noticeable method to remind you to read the privacy policy when you first use the application? If yes, please describe it.
    (a) You said that "I will read the privacy policy update announcement" in the pre-survey, so what content do you focus on?
        (i) Did the application publish the privacy policy update announcement after the implementation of PIPL? Have you read it?
        (ii) Have you noticed the changes in the privacy policy in informed consent after the implementation of PIPL? If yes, please detailed describe it.
    (b) You said that "I don't care about the privacy policy at all" in the pre-survey. What is the reason?
    (c) What measures could better help catch the information in the privacy policy? Why do you think the measure is effective?
(16) Except for the above information collection methods, are there any other ways that you learn about how the application uses and collects personal information? If yes, please detail describe it.
    (a) Could you find the personal information collection list in the application? Please screen-record the process.
    (b) What opinion do you have about the personal information collection list?
    (c) Is there any information collected that you didn't expect? If yes, please describe it.
    (d) What measures do you think could improve the personal information collection list?
    (e) When you encountered trouble in the personal information collection list, did you try to ask customer service? If yes, please describe it.
(17) How do you think the application would use to get your consent during personal information collection?
    (a) What is the individual's separate consent?
    (b) Among the above ways mentioned, which ways do you think are going to be used to obtain your individual separate consent?
    (c) Except for the above cases, what case do you think needs your individual's separate consent?

   (d) PIPL regulated that processing sensitive personal information must request the related individual separate consent. So what information do you think belongs to sensitive personal information? Why do you think so?
   (e) Do you think the application's action of requesting your individual separate consent has increased? If yes, please describe it.
   (f) Do you think the individual separate consent is helpful for personal information protection? If yes, please describe it.

(18) Besides the above individual separate consent, do you think there are other special ways to request consent to process your information? If yes, please describe it.
   (a) PIPL regulated the cases that need to obtain your individual's separate consent again, for convenience, I will call it renewal consent in the following questions. What do you think renewal consent is?
   (b) In the above-mentioned case, which case do you think belongs to re-obtaining your individual separate consent?
   (c) Is there any other case related to re-obtaining your individual separate consent? If yes, please describe it.
   (d) In what case do you think a personal information processor needs to re-obtain your individual separate consent?
   (e) What is the effect of the renewal consent?

(19) PIPL regulates that an information processor could directly take your information by waiving your consent in emergencies. In what emergency do you think the information processor could directly collect your personal information? What do you think about it?

(20) Do you find that any non-compliance behaviors in the application violate your informed consent? If yes, please describe it.

(21) Have you had the experience that your informed consent was violated by the application? If yes, Please describe it.
   (a) What do you think about the violation?

(22) Have you had the experience that it was hard for you to execute the right to know?
   (a) If yes, what difficulty did you encounter? or what difficulty do you think you may encounter?
   (b) How do you overcome the difficulty?

APPENDIX C - INTERVIEWEE RESPONSES

Table C1. Interviewees' responses, general awareness of PIPL, and attitudes towards PIPL and privacy.

Question	Responses
In November 2021, the Personal Information Protection Law (PIPL) came into effect in China. Have you heard of PIPL?	• Yes, and I know what it means: 4 (13.3%) • Yes, I know a little, but not enough about what it means: 16 (53.3%) • Yes, but I do not know what it means: 8 (26.7%) • I have never heard of it: 2 (6.7%)
PIPL clarified individuals' rights when using personal information processors. What do you think about this?	• I think my rights have improved: 8 (26.7%) • I don't think my rights have improved: 13 (43.3%) • I don't care at all: 2 (6.7%) • I do not know: 7 (23.3%)
To what extent do you take measures to protect your personal information while using applications in your daily life? (5 point scale)	• 5: 3 (10%) • 4: 9 (30%) • 3: 9 (30%) • 2: 8 (26.7%) • 1: 1 (3.3%)
When you download a new mobile application, you need to accept its privacy policies to use it. How do you react to these privacy policies?	• I always read the whole privacy policy though it takes a lot of time: 5 (16.7%) • I always go through the privacy policy but only focus on some highlights or the terms I am concerned about: 6 (20%) • Sometimes I check the privacy policy. It depends on whether I have time or on the platform I use: 10 (33.3%) • I consent to the the privacy policy without reading it: 9 (30%)

Received January 2023; revised July 2023; accepted November 2023