Security Risks and Governance of User Personal Information on Online Information Service Platforms: A Postprint Based on Content Analysis of 117 APP Privacy Policies

Authors: Liu Yu, Zhou Yi, Nong Yanqing

Date: 2023-04-01T15:51:23+00:00

Abstract

[Purpose/Significance] While network information service platforms provide substantial convenience for public production and daily life, the problem of personal information leakage among platform users is becoming increasingly severe. Exploring these risks and implementing effective governance serves as a critical lever for enhancing cyberspace governance capabilities and promoting the modernization of the governance system.

[Methods/Process] Through cluster analysis of privacy policy content from 117 sample App platforms, this study identifies potential risk types related to user personal information security.

[Results/Conclusion] The micro-ecosystem of third parties in the network information service process, the internal ecosystem of network information service platforms, and the external ecosystem of industry associations of network information service platforms collectively constitute the overall ecological environment of cyberspace. This paper proposes relevant approaches for strengthening the governance of user personal information security risks from the perspectives of platform privacy policy formulation, platform internal control mechanisms and third-party interaction mechanisms, and the exertion of government governance roles.

Full Text

Preamble

Network Information Service Platform Users' Personal Information Security Risks and Their Governance: A Content Analysis Based on 117 APP Privacy Policy Texts

Liu Yu[1], Zhou Yi[2], Nong Yanqing[2]
[1]School of Politics and Public Administration, Soochow University, Suzhou 215123
[2]School of Sociology, Soochow University, Suzhou 215123

Abstract: [Purpose/Significance] While network information service platforms provide great convenience for public production and life, the problem of user personal information leakage is becoming increasingly serious. Analyzing these risks and implementing effective governance is crucial for enhancing cyberspace governance capacity and modernizing the governance system. [Method/Process] Through cluster analysis of privacy policy content from 117 sample App platforms, this study identifies potential risk types for user personal information security. [Result/Conclusion] The third-party micro-ecology in network information service processes, the internal ecology of network information service platforms, and the external ecology of network information service platform industry groups collectively constitute the overall ecological environment of cyberspace. The paper proposes governance approaches to strengthen user personal information security risk management from three aspects: platform privacy policy formulation, platform internal control mechanisms and third-party interaction mechanisms, and the role of government governance entities.

Keywords: network information service platform; user personal information; security risk; governance
Classification Number: G203
DOI: 10.13266/j.issn.0252-3116.2022.05.004

---

1 Research Background

1.1 Real-World Context

Recently, Didi Chuxing was removed from app stores by the Cyberspace Administration of China for illegally and excessively collecting users' personal privacy. Prior to this, numerous mobile Apps had been exposed for similar problems, with platforms employing increasingly diverse methods to collect user information, thereby escalating network information security risks. According to Ministry of Industry and Information Technology data, by the end of February 2021, there were 3.28 million network information service platforms (primarily various Apps) in the domestic market. While these Apps bring tremendous convenience to people's work and life, user personal information protection issues have become increasingly prominent. As the main body of network information services, Apps possess a unique dual nature that endows them with a special mission and critical node role in network information security risk governance. Therefore, strengthening App personal information protection is imperative.

The publication and effective implementation of App privacy policies have played a positive role in improving user personal information protection and

represent an effective approach to alleviating user privacy concerns. However, various Apps exhibit numerous problems in both privacy policy text content and implementation effectiveness, which seriously disrupt the healthy order of cyberspace, harm the legitimate rights and interests of the people, and even pose potential threats to national security.

1.2 Research Progress

Literature review reveals that current research on user privacy policies in network environments primarily focuses on three aspects: personal privacy protection system design, privacy policy content expression and analysis, and privacy policy application and practice.

1.2.1 Personal Privacy Protection System Design Research China's *Data Security Law* and *Personal Information Protection Law* took effect on September 1, 2021 and November 1, 2021, respectively. Prior to this, academic research on network platform personal privacy protection system design was relatively concentrated. Zhou Yi proposed improving governance mechanisms from the perspective of network information content ecological security governance, suggesting the formation of multi-stakeholder governance synergy, establishment of relief mechanisms, clarification of the sources of service platform management authority, and enhancement of service platform governance capacity to achieve transformation from passive control to active construction of network information content ecological security, from expedient campaign-style governance to normalized participatory governance, and from focusing on action processes to focusing on action effectiveness. Zhang Linghan, based on the platform automated decision-making governance framework established in the *Personal Information Protection Law (Draft)*, proposed that legislators should update the traditional legal accountability approach of "subject-behavior-liability" with a technical governance mindset. Zhu Gaofeng clarified the attribution principles and liability 承担 methods for artificial intelligence infringement of personal information rights, pointing out the need to actively formulate industry standards and establish personal privacy protection systems and user choice systems in the AI field. Yang Jianguo argued that addressing the ethical dilemmas of privacy protection in the big data era requires reconstructing technological ethics and promoting the unity of instrumental rationality and value rationality. Li Xin contended that relying solely on personal information protection legislation is insufficient to address current dilemmas; mandatory national standards should be established to define the form and essential content of privacy agreements, combining transparency with daily reporting, and strengthening personal information protection through public-private parallel approaches. Zhang Yong distinguished between weak protection of personal information rights and strong protection of privacy rights, noting that the latter involves core aspects of citizens' personality dignity, and that while general personal information can often be collected without explicit consent, private sensitive information should be protected by privacy rights rather than merely through informed con-

sent. Ding Fengling argued that collective data governance models represent an optimal choice, with data trusts effectively addressing inequality in the data economy through bottom-up group autonomy. Gong Tao proposed establishing an opt-out mechanism for targeted advertising that combines opt-in and opt-out approaches, based on distinguishing between non-personal information, general personal information, personal sensitive information, and various types of messages and advertisements. Wang Yegang pointed out that privacy policies without user consent belong to purely corporate self-discipline rules that cannot establish contractual relationships between network service providers and users, and that such policies have no binding effect on users regarding personal information collection and utilization.

1.2.2 Privacy Policy Content Expression and Analysis Research Some scholars have proposed optimization suggestions for platform privacy policy text content through large-sample text analysis. Xu Lei analyzed 55 Chinese and 20 English mobile App privacy clauses, noting that current mainstream privacy clauses suffer from poor accessibility and lack initiatives to enhance user engagement. Guo Qingyue et al. analyzed 200 commonly used Apps' privacy policies and found that current App privacy policies primarily consist of three components—the personal information protection subject, App business functions, and personal information processing behaviors—which tend to omit details and lack expandability. They proposed optimizing the App privacy framework using a three-dimensional coordinate system structure that incorporates personal information processing behaviors, specific App business functions, and multi-stakeholder connections in personal information protection. Yao Shengyi et al., from a user perspective, proposed App privacy policy user-friendliness as an evaluation direction. Through systematic research on domestic and international personal information protection policies, Zhan Nan proposed building a new path for personal information protection with Chinese characteristics by establishing specialized personal information protection agencies, constructing integrated protection systems for prevention, emergency response, and relief, and improving government-led social collaborative protection supervision mechanisms. K. Martiny et al. introduced a privacy protection strategy framework that builds privacy policy decision paths to achieve interaction with users and privacy policy verification and management. S. T. Wang found, through analysis from the perspectives of user brand awareness and social norms, that users with more positive attitudes toward privacy policies are more willing to self-disclose during use. Yu Jianan pointed out that when platform mergers and other commercial behaviors occur, user data transfer should be permitted if both parties have reasonable interests, but users should be given the right to make contrary choices beforehand or afterward. These studies identify deficiencies and hidden dangers in current platform privacy policies and propose optimization suggestions from user perspectives.

1.2.3 Privacy Policy Application and Practice Research As digital transformation accelerates, network information service platforms have become ubiquitous and all-powerful in public life, prompting scholars to examine platform privacy policy practices. Zhou Linxing et al. proposed personal information governance strategies from four dimensions: multi-governance, technical governance, corporate governance, and user governance. Chen Bing et al. suggested expanding the focus of data protection from the data collection stage to the data usage stage to improve deep data value mining and innovative application of data technologies. Jin Yuanpu analyzed the attributes, causes, and hazards of leaked data through big data, pointing out that privacy protection and data leakage prevention require reforms in systems, mechanisms, communication, and education. In the social platform domain, Yuan Xiangling et al. noted that social media should inform users about privacy information usage and processing procedures through privacy policies, which can enhance user trust in social media and strengthen users' self-disclosure willingness. In library services, Guo Jun proposed constructing a library user personal information protection framework comprising four modules: pre-event prevention, in-process control, post-event accountability, and legislative regulation. Xu Lei et al., from the perspective of book category App privacy policy text research, proposed improving existing privacy policies and protecting reader personal information by enhancing reader participation in privacy policy formulation and revision, increasing privacy policy visibility and accessibility, consolidating the legal foundation of privacy policies to promote iterative optimization, improving privacy policy quality with attention to minors' information protection, and building a multi-stakeholder collaborative governance system to ensure privacy policy implementation. In new technology application fields, Xu Guimin et al. conducted an intelligent deconstruction of crimes such as illegal web scraping of personal information, platform forced overreach, malicious Apps, and mobile information theft from a multi-dimensional technological perspective. Regarding users' right to be forgotten, Liu Xuetao et al., based on considerations of the necessity of localizing the right to be forgotten, proposed "promoting the implementation of existing legal norms and treating legislation on the right to be forgotten with caution." Foreign scholars have conducted earlier research in privacy policy application and practice. J. H. Smith et al. proposed in the APCO (Antecedents→Privacy Concerns→Outcomes) theoretical model that privacy policies are positively correlated with self-disclosure. The APCO model was the first to systematically elaborate the mechanism of privacy policies' effect on self-disclosure, emphasizing a multidisciplinary, macro perspective on information privacy issues and focusing on correlations between variables. M. Boldt et al. analyzed privacy policy texts of the world's top 100 Fortune companies to discuss differences between legitimate and malicious privacy policies. These studies provide multi-angle systematic analysis based on current platform applications and privacy policy requirements across various dimensions.

In the aforementioned research, sample analysis and empirical studies provide a practical foundation for platform personal privacy protection system design;

application and practice research offers corresponding feasibility guarantees for platform privacy policy optimization; and privacy policy content research integrates relevant theories, methods, and technical applications, guiding theoretical and technical research with practical problems. These three aspects complement each other, forming a complete spiral research system.

1.3 Problem Statement

Through analysis of privacy policy texts from 117 Apps across 39 categories, this study finds that current network information service platform user personal information security risks primarily manifest at three levels: individual users, social development, and national security. Individual user risks are reflected in App users' tendency to "self-abandon" when facing privacy terms by directly agreeing to them, gradually turning information subjects into information puppets. Social development risks are reflected in platforms placing the public in "information cocoons," "data islands," and "transaction mazes," making platform data collection and usage difficult for the public to question or supervise, thereby turning platforms into lawless zones in the network world. National security risks are reflected in the possibility that network information service platforms with massive citizen personal information may become generators and transformers of national core information, bringing potential national security hazards. This study conducts empirical research and analysis on network information service platform user information security risks, exploring feasible governance strategies from the perspectives of the public individual, platform groups, and the national whole, with the main goal of achieving multi-stakeholder governance of network information service platform user personal information security risks.

---

2 Research Path and Results Analysis

2.1 Sample Selection

This study examines platforms' "User Privacy Regulations" or "User Privacy Terms" from the perspectives of legality and rationality, extracting key information from privacy clauses of different platforms regarding user privacy, third-party data open authorization, and SDK usage, with particular focus on 梳理 ing situations where platforms share user information with third parties, third-party software developers (ISV), and data service software development kit (SDK) providers when delivering services and goods to users. By comparing App download rankings in various app stores including App Store and Tencent Appstore, this study selected the top three Apps in each category. After excluding inaccessible Apps, those without posted privacy policies, and duplicate privacy policies, 117 Apps were ultimately selected, including WeChat, TikTok, Tencent, and Keep, with total privacy policy text reaching 1.48 million characters.

2.2 Research Methods

Sample Apps' privacy policy texts contain certain inductive keywords, whose frequencies can reflect platforms' security risk levels regarding user privacy, third-party data open authorization, and SDK usage. This study employs cluster analysis and content analysis methods to extract key information from major service platforms' privacy clauses, using ROSTCM6 for text data processing and content analysis to analyze sample Apps' privacy policies. By comparing keyword frequencies, the study identifies platforms' hidden security risk situations.

2.3 Statistical Results

Based on the "Regulations on the Scope of Necessary Personal Information for Common Types of Mobile Internet Applications," common Apps are divided into 39 categories. This study selected the top three Apps by market share in each category as sample objects, obtaining user privacy clauses through multiple channels. After compilation, 117 privacy clauses were collected, as detailed in Table 1 . After deep mining of privacy policy texts using ROSTCM6, main terms were filtered out, as shown in Table 2 . Substituting these main terms into policy texts for interpretation yielded results and analysis presented in Table 3 .

Overall statistical results show concentrated risk issues in the total sample, as presented in Table 4 . Categorized statistical results reveal main risk issues for different App types, as shown in Table 5 .

2.4 Sample Results Analysis

Based on statistical analysis of concentrated risk issues in the total sample and main risk issues across App categories, this study finds that hidden personal information security risks in App privacy policies mainly include four categories: (1) platform privacy policies inducing user authorization; (2) platforms restricting user rights protection through technical barriers; (3) platforms' profit-driven nature exposed in management processes; and (4) platforms colluding with third-party institutions to create regulatory blind spots.

2.4.1 Platform Privacy Policy Induces User Authorization This includes: (1) The "privacy-for-service" problem. To complete identity verification, confirm transaction status, and provide after-sales service and dispute resolution, platforms can obtain users' personal information from third parties. (2) Platforms' clever risk-avoidance clauses. When users employ third-party services through the platform, third-party privacy regulations apply or the platform provides third-party links but makes no guarantees about third-party platforms' privacy security. When users authorize platforms to share personal information with third parties, those third parties' privacy protection policies apply. (3) Potential hazards of third-party personal information usage. Platforms access third-party service providers through third-party account login, sharing content

to third-party products, etc., and can provide user information to third parties under users' tacit consent, while indirectly obtaining corresponding (derived) information from third parties.

2.4.2 Platform Restricts User Rights Protection Through Technical Barriers This includes: (1) Usage barriers created by technical fences. Although platforms allow users to manage or delete Cookies according to their preferences, doing so requires users to change settings during every website visit, increasing usage difficulty. (2) Restriction of users' "right to deletion." While platforms allow users to access, correct, or delete relevant information upon request, they must retain personal information for legitimate reasons. (3) Personal information used to improve platform marketing strategies. When users employ platform products, third-party service providers and advertising partners automatically collect certain user-related information through user local terminal data (Cookies) and tracking technologies, including IP addresses, browser types, ISP, referral URLs, exit pages, files viewed on platform sites, operating systems, date/time stamps, and/or clickstream data, which platforms use to improve their marketing efforts.

2.4.3 Platform and Third-Party Institutions Collude to Create Regulatory Blind Spots This includes: (1) Platforms sharing user information with third parties. When transactions such as mergers, acquisitions, or asset transfers result in sharing users' personal information with third parties, platforms only inform users of relevant situations through push notifications, announcements, and other forms. (2) Platforms and third parties colluding to obtain user personal information. Platform products contain third-party SDKs or similar applications. When users employ such third-party services on platforms, they are required to allow third parties to collect and process user information through embedded code, plug-ins, and other forms. For example, when users pay with Alipay, the Alipay SDK needs to read users' International Mobile Equipment Identity (IMEI) information to enable transactions in a secure environment. In such cases, third-party service providers' information collection and processing behaviors comply with their own privacy terms rather than the platform's privacy policy. (3) Personal information acquisition in platform service outsourcing. Due to the lack of institutional design for personal information entrustment processing in domestic laws and regulations, the implementation of data security responsibilities for a large number of customer service outsourcing arrangements, third-party software developers (ISV), and data service software development kits (SDK) remains in a gray area. Additionally, due to different types of specific goods and services, e-commerce may involve multi-industry regulatory issues, with problems such as multi-head regulation and unregulated gray areas existing to varying degrees.

2.4.4 Platform's Profit-Driven Nature Exposed in Management Process This includes: (1) Information leakage risks among platform internal

personnel. Weak internal network security precautions, insufficient professional ethics education and confidentiality training for employees with confidentiality obligations, and internal employees leaking user personal information for profit increase information security risks. (2) Platforms' universalization of inducing user authorization to use information. Platforms share information with promotion and advertising partners without identifying individuals to improve advertising reach and effectiveness. (3) Platforms processing user information to detect potential consumption needs. Platforms collect user information through Cookies and Web Beacons, and after statistical processing, provide it to advertisers or other partners for analyzing how users employ platform services, using relevant information for advertising push services. (4) Platforms associating information across different internal products and services to achieve user profiling. When using platform services, users are redirected to other service interfaces provided by the platform, which provides user information to different internal product and service channels for account association. If users refuse platform collection of such information, their use of platform core business functions and additional business functions will be affected.

Through the above analysis, the internal logical relationships of the four categories of security risk issues can be represented as: third-party issues (micro-ecology) → platform internal management mechanism issues (internal ecology) → network information service platform industry group issues (external ecology) → domestic network overall ecological governance issues (macro-ecology). The problem of platforms colluding with third-party institutions to create regulatory blind spots (Risk A) affects the third-party micro-ecology and platform internal management ecology; the problem of platforms' profit-driven nature exposed in management processes (Risk B) affects the platform internal management ecology and network information service platform industry group external ecology; the problems of platforms restricting user rights protection through technical barriers (Risk C) and platforms inducing user authorization through privacy policies (Risk D) affect the platform internal management ecology, network information service platform industry group external ecology, and domestic network overall macro-ecology. The impact of various information security risks on information security ecology 各环节 is illustrated in Figure 1 [Figure 1: see original paper].

Through analysis of various Apps' privacy policy texts, this study extends from problems existing in third-party institutions associated with platforms involving user privacy, third-party data open authorization, and SDK usage, to problems such as App platforms inducing user authorization in privacy policies, restricting user rights protection through technical barriers, colluding with third-party institutions to create regulatory blind spots, and exposing profit-driven nature in management processes, thereby exploring governance strategies from the dimensions of the platform's overall external environment and the current network space macro-ecology.

3 Causes and Governance Strategies for Personal Information Security Risks on Network Information Service Platforms

3.1 Causes of Personal Information Security Risks on Network Information Service Platforms

3.1.1 Insufficient Legal Basis for Governance Although a series of laws and regulations including the *Cybersecurity Law* have been enacted at the national level, problems remain regarding insufficient legal support for personal information protection. Current laws and regulations have unclear definitions of user information infringement subjects, face difficulties in obtaining evidence for user information infringement, and have imperfect relief channels for user information infringement, resulting in increasingly lower costs for collecting user personal information and increasingly higher precision in personal information infringement against target objects, causing severe information threats to individual users.

3.1.2 Profit-Driven Nature of Platform Groups The data-is-king development concept of some network information service platforms prevails within the industry, with inadequate self-regulation mechanisms in platform industry groups, and behaviors infringing upon user rights and even violating laws and regulations occurring frequently. Some platforms rely on their scale and strength to set market entry barriers, monopolize user resources, collect massive amounts of information, accurately understand consumers and their needs, and thereby target service or product delivery. To circumvent platform risks, platforms transfer service projects to third parties to optimize operating costs, thereby shifting personal information security risks.

3.1.3 Absence of Network Community Role Rogers' Protection Motivation Theory posits that when people face threats, their protective behaviors are based on two considerations: threat appraisal and coping appraisal. When coping appraisal is lower than threat appraisal, subjects are inhibited from adopting protective behaviors. Currently, network users' awareness of actively adopting information security measures to avoid and respond to information security threats is relatively weak, resulting in low response efficacy, and the overall coping efficacy of network communities is also not significant. This leads network communities to exhibit characteristics of conceptual fragmentation, value dispersion, and identity separation, with collective action in communities continuously declining. The reason is that network communities or network social organizations have not fully leveraged their advantages, integrated network resources, or mobilized network forces to resist network platforms' infringement of user information rights, failing to realize their important role as bridges and links between government, platforms, and users, which to some extent encourages the spread of platforms' infringement of user personal information rights.

3.2 Governance Strategies for Personal Information Security Risks on Network Information Service Platforms

Based on the above analysis, strengthening governance of user personal information security risks on network information service platforms should focus on three aspects: improving the platform privacy policy framework, optimizing platform internal information management mechanisms, and strengthening the role of government governance entities.

3.2.1 Improving the Platform Privacy Policy Framework

(1) **Develop Universal Privacy Clauses for Various Platforms.** Government-led network information service platform industry groups should formulate universal privacy clauses for network platforms to reduce users' burden of reading various App privacy clauses. Based on different business needs of various network platforms, universal privacy clauses should be formulated by category, focusing on clarifying rights and obligations between platforms and users, information collection scope, and information utilization and reuse standards. These clauses must be dynamically and hierarchically approved by users when registering, using associated services, and cooperating with third parties to maximize user choice. If differences exist between service platform clauses and national universal privacy clauses, platforms are obligated to explicitly inform users to protect their right to know.

(2) **Improve Platform Privacy Policy Consent Systems.** On one hand, eliminate presumed consent; consent must be direct and explicit. Platform privacy policies should delete erroneous provisions such as "using the software means agreeing to the privacy policy," because user consent under such circumstances cannot exclude the possibility of defects in the privacy policy. Platform-obtained user consent should be based on users' complete reading and must involve genuine and clear expressions of user intent. Therefore, privacy policies with specific content and concise expressions are more likely to attract users to read actively, and only user consent based on such reading has legitimacy. On the other hand, eliminate induced consent; consent must be confirmed clearly. When users first use an App, the login and registration interface should inform users of personal information processing and usage rules in a concise and clear manner, including information processing subjects, purposes, forms, storage duration, and sharing permissions. When users refuse App authorization requests, platforms must not force users to exit or automatically close the software, must not induce user consent to privacy policy content by opening service content, must not apply for user authorization beyond current service scope and service items in advance, must not repeatedly apply for information permissions beyond current service scope through pop-up windows, must not automatically use and associate third-party Apps for non-service scope and irrelevant scenarios, and must not stop users from

enjoying basic services due to their refusal to authorize.

(3) **Improve Platform Rules for Collecting User Information.** Platforms should inform users of rules for collecting and using their personal information in a direct, accurate, comprehensive, and clear manner. These rules should include basic content such as the scope, form, purpose, and frequency of user information collection, as well as protection measures for user information desensitization, disclosure, sharing, and destruction, ensuring users' right to know and choose. Platforms must strictly fulfill their duty to inform users before collecting personal information, obtaining explicit user confirmation before initiating services. Platforms must strictly regulate targeted advertising based on user information, prohibiting advertising precision placement or marketing activities based on user profiling without clear user notification and consent, truly purifying the network information service platform environment.

(4) **Improve User Information Hierarchical Dynamic Management Systems.** User information on network platforms can be divided into three levels: Level 1 is personal privacy information that individuals do not want to be illegally collected, probed, or disclosed, falling within privacy rights protection scope; Level 2 is personal identity information indicating user identity characteristics, including ID numbers, home addresses, contact information, and account information; Level 3 is derived data, which is information formed after processing massive amounts of personal information stored on networks, produced after desensitizing personal identity information (Level 2). In system operation, attention should be paid to building communication channels between network platforms and users to ensure standardized classification management and use of continuously increasing user information storage on the premise of continuous user authorization. Simultaneously, platforms should establish and improve dynamic management and continuous disclosure systems for information utilization, enabling users to track personal information collection and use throughout the process and make different authorizations according to changes in platform services or product offerings. The platform information dynamic management system requires platforms to allow users to readjust their authorizations based on changing service needs and product requirements; the platform information utilization continuous disclosure system requires platforms to continuously inform users about what information has been used, how it was used, and what value was generated, providing users with regular reports on information collection and utilization.

3.2.2 Optimizing Platform Internal Information Management Mechanisms

(1) **Optimize Platform Internal Control Mechanisms.** Network information service platforms should explore management models more suit-

able for themselves and strengthen monitoring of information security risks. Platforms should formulate scientific internal control mechanisms, build internal risk control systems and platform internal control systems, and regularly assess platform information risks to avoid problems such as user information leakage. Platforms should establish complete internal control organizational structures, with internal control departments conducting strict reviews of platform-related software and hardware, strengthening confidentiality management of business personnel in platform system development, operation, and maintenance departments, and cultivating confidentiality and risk control awareness among all platform staff. Simultaneously, platforms should establish standardized processes and exception handling procedures for personal information security risk management to ensure risk control measures can be applied to manage platform personal information security risks when emergencies occur.

(2) **Optimize Collaborative Mechanisms for Manual and Intelligent User Information Screening.** Platform user information screening includes three stages: pre-event, in-process, and post-event. Pre-event screening primarily targets compliant user information collection; in-process screening focuses on legal user information desensitization; post-event screening is mainly used for user data utilization and reuse. In the era of rapid AI development, platforms should pay attention to algorithmic discrimination and technical loopholes in intelligent screening that require manual regulation, leveraging the respective advantages of manual and intelligent screening and combining them with the characteristics and requirements of each stage of platform user information screening to innovate collaborative mechanisms. Pre-event screening involves large volumes of user information collection with high compliance requirements and serves as the foundation for platforms to provide targeted services, thus can be primarily intelligent; in-process screening mainly includes target information pool optimization and service construction, which have higher legality requirements and should be primarily manual; post-event screening focuses on serving user data utilization and reuse, involving large information volumes and high service standards, and can be achieved through collaboration between manual and intelligent screening. Under the collaborative screening mechanism, manual and intelligent screening each demonstrate their strengths, achieving comprehensive optimization of platform services according to different user information processing requirements and precision standards at different stages with differentiated emphasis and coordinated operation.

(3) **Optimize Platform and Third-Party Information Sharing Mechanisms.** Although platforms provide convenience to users through third-party services, third-party institutions may also use their technological advantages to steal and leak user personal information, thereby infringing upon user privacy rights. Platforms should clarify their status as respon-

sible subjects for network information services, fulfill their responsibilities in protecting user personal information when jointly conducting information services with third-party institutions, and form and improve information sharing mechanisms with third parties. On one hand, platforms should clarify information sharing boundaries with third parties, discovering critical points for different information sharing based on balancing personal privacy rights and public interests to determine the extent to which third-party platforms can expand user information collection and utilization and where this expansion's boundaries lie. On the other hand, platforms should improve relief mechanisms when user information rights are infringed. When user personal information is infringed, users usually do not discover it immediately, while third parties, based on their technological advantages, often first discover the fact of user information infringement. Therefore, third parties have an obligation to provide timely remedies when discovering user information infringement. Remedy mechanisms mainly include: using technical means to track and protect leaked or stolen information; third parties promptly informing users of the real situation and remedy progress; and reporting information infringement and obligation fulfillment to platforms and regulatory authorities to achieve effective remediation.

3.2.3 Strengthening Government's Role as Governance Entity

(1) **Ensure Effective Implementation of Information Security Laws.** With the implementation of the *Personal Information Protection Law*, infringement of personal information security will be fundamentally regulated. In implementing the *Personal Information Protection Law*, attention should be paid to improving online and offline collaborative protection mechanisms for user information; in personal information collection, clearly requiring platforms to adopt minimum scope information collection principles even with user authorization, strictly prohibiting platforms from affecting service quality due to user refusal to authorize; improving relief mechanisms for user personal information infringement, clarifying legal responsibilities of infringers; establishing a national-level user information infringement reporting platform that clearly defines information collection sources, scope, behaviors, and relief measures of reported parties; and implementing provisions in the *Personal Information Protection Law* concerning users' "right to be forgotten" to effectively constrain network information service platforms' data collection, utilization, and deletion behaviors.

(2) **Improve Legal Liability Pursuit Systems.** Establishing a complete legal liability pursuit system helps protect users' personal information rights, clarifies the competent authorities for network information service platform user personal information protection, and ensures that when user personal information infringement occurs, relevant authorities actively par-

ticipate in users' accountability and compensation activities during the relief-seeking process, lowering the threshold and difficulty of user rights protection. An open and transparent infringement relief procedure should be established. When users initiate complaints against platform infringement, competent authorities should conduct legitimacy and legality reviews of complaints, fully participate in subsequent relief processes, ensure lawful, transparent, and open procedures for initiation, investigation, hearing, decision, and execution, require platforms to provide feedback on handling results according to regulations, and take necessary measures such as deletion, blocking, and disconnection as appropriate to ensure thorough implementation of legal liability pursuit systems. A complete supervision mechanism should be established to ensure platforms use user information more legally and compliantly, reducing information acquisition desires driven by subjective profit-seeking and effectively ensuring that infringed users can conduct legal and effective infringement compensation.

(3) **Establish Specialized Government Management Agencies.** The Cyberspace Administration of China, Ministry of Industry and Information Technology, Ministry of Public Security, and National Administration of State Secrets Protection are all competent authorities for network information security. This multi-head governance model cannot truly improve national network information comprehensive governance capacity or effectively promote the healthy development of network information governance issues through national will. Network information service platform governance involves games among multiple interest stakeholders, requiring the construction of a new governance relationship with government functional departments at the core and network platforms, social organizations, and netizens as multiple participating entities. Drawing on national-level network information protection agencies established in countries such as Brazil, a specialized agency could be established to 专职 handle and coordinate all matters related to personal information protection for network information platform users. The agency would manage and supervise platforms that have collected or are collecting network user personal information, guide and regulate platforms' use of citizen information for commercial services, and realize the positive role of network information in promoting economic and social development while fully protecting user personal information rights.

References

[1] Chen Yao. Why Personal Information Leakage Occurs Frequently [EB/OL]. [2020-12-29]. http://www.ccdi.gov.cn/yaowen/202012/t20201229_{232770}.html.

[2] Notice on the Situation of 33 Apps Including Input Method Apps Illegally

and Irregularly Collecting and Using Personal Information [EB/OL]. [2021-05-01]. http://www.cac.gov.cn/2021-04/30/c_{1621370239178608}.htm.

[3] Liu Bailing, Wan Lulu, Li Yanhui. A Review of Privacy Protection Research Based on Privacy Policies in Network Environment [J]. Information Studies: Theory & Application, 2016, 39(9): 134-139.

[4] Zhou Yi. On the Construction of Network Information Content Ecological Governance Mechanism [J]. Journal of Intelligence, 2020, 39(12): 96-101.

[5] Zhou Yi. On the Composition of Network Information Content Governance Subjects and Their Action Transformation [J]. E-Government, 2020(12): 41-51.

[6] Zhang Linghan. Platform Algorithm Accountability System in the Personal Information Protection Law (Draft) and Its Improvement [J]. Review of Economic and Trade Law, 2021(1): 36-46.

[7] Zhu Gaofeng. On Legal Protection of Personal Information Security in Artificial Intelligence Field [J]. Journal of Chongqing University (Social Science Edition), 2020, 26(4): 150-160.

[8] Yang Jianguo. Formation Mechanism and Governance of Privacy Protection Ethical Dilemma in Big Data Era [J]. Jiangsu Social Sciences, 2021(1): 142-150, 243.

[9] Li Xin. Protection Path of Personal Information in Privacy Agreements in Big Data Era—From the Perspective of Internet Stratification [J]. Journal of Soochow University (Philosophy & Social Science Edition), 2020, 41(3): 77-87.

[10] Zhang Yong. Criminal Law Protection of App Personal Information: From the Perspective of Informed Consent [J]. Law Science, 2020(8): 113-126.

[11] Ding Fengling. Choice of Personal Data Governance Model: Individual, State, or Collective [J]. Journal of Huazhong University of Science and Technology (Social Science Edition), 2021, 35(1): 64-76.

[12] Gong Tao, Guan Zhaoyu. Principle, Jurisprudence, and Governance of Targeted Advertising [J]. Journal of Taiyuan University of Technology (Social Sciences Edition), 2021, 39(1): 60-67.

[13] Wang Yegang. On the Effectiveness of Network Privacy Policies—Centered on Personal Information Protection [J]. Journal of Comparative Law, 2020(1): 120-134.

[14] Xu Lei, Xu Runjie. Research on Accessibility and Content Analysis of Mobile App Privacy Clauses [J]. Modern Information, 2020, 40(7): 82-91.

[15] Guo Qingyue, Wu Dan. Research on Optimization of App Privacy Policy Framework Based on Text Analysis [J]. Journal of Information Resources Management, 2021, 11(1): 18-29.

[16] Yao Shengyi, Wu Dan. Research on User Friendliness Evaluation of App Privacy Policies [J]. Journal of Information Resources Management, 2021, 11(1):

30-39, 58.

[17] Zhan Nan. Research on Domestic and International Personal Information Protection Policy System [J]. Library and Information Service, 2019, 36(5): 120-129.

[18] Martiny K, Elenius D, Denker G. Protecting Privacy with a Declarative Policy Framework [C]//IEEE International Conference on Semantic Computing. Laguna Hills: IEEE, 2018: 227-234.

[19] Wang S T. Effects of Brand Awareness and Social Norms on User-Perceived Cyber Privacy Risk [J]. International Journal of Electronic Commerce, 2019, 23(2): 272-293.

[20] Yu Jianan. Personal Information as Corporate Assets—Balancing Personal Information Protection and Operator Rights in Corporate Mergers [J]. Global Law Review, 2020, 42(1): 99-112.

[21] Zhou Linxing, Han Yongji. Research on Personal Information Governance in Big Data Environment [J]. Information Science, 2021, 39(3): 11-18.

[22] Chen Bing, Ma Xianru. Discussion on User Data Protection Approaches in Internet Era [J]. Journal of Northeastern University (Social Science), 2021, 23(1): 96-104.

[23] Jin Yuanpu. Investigation and Analysis Report on Personal Privacy Data Leakage in Big Data Era [J]. Journal of Tsinghua University (Philosophy and Social Sciences), 2021, 36(1): 191-201, 206.

[24] Yuan Xiangling, Niu Jing. Empirical Research on Social Media Privacy Policies and User Self-Disclosure: A Moderated Mediation Model [J]. Journal of Information Resources Management, 2021, 11(1): 49-58.

[25] Guo Jun. Research on Library User Personal Information Protection in Big Data Environment [J]. Library Work and Study, 2020(1): 11-19, 28.

[26] Xu Lei, Guo Xu. Practical Logic and Normative Path of Reader Personal Information Protection in Big Data Era—From the Perspective of Book Category App Privacy Policy Texts [J]. Library Development, 2021(1): 74-83, 92.

[27] Xu Guimin, Zhang Zhuan. Intelligent Deconstruction, Interpretation, and Regulation of Illegal Acquisition of Citizen Personal Information Behavior—Based on Multi-Dimensional Technology Aspects [J]. Journal of Chinese People's Public Security University (Social Sciences Edition), 2020, 36(6): 130-142.

[28] Liu Xuetao, Li Yue. Consideration of Localizing the Right to Be Forgotten in Big Data Era—From the Perspective of Comparison with Personal Information Deletion Right [J]. Science Technology and Law, 2020(2): 78-85.

[29] Smith J H, Dinev T, Xu H. Information Privacy Research: An Interdisciplinary Review [J]. Social Science Electronic Publishing, 2011, 35(4): 989-1015.

[30] Boldt M, Rekanar K. Analysis and Text Classification of Privacy Policies from Rogue and Top-100 Fortune Global Companies [J]. International Journal of Information Security and Privacy, 2019, 13(2): 47-66.

[31] Wang Luyao, Li Qi, Qiao Zhilin, et al. Research on the Influence of Protection Motivation on Social Network Users' Privacy Concerns and Privacy Security Protection Behavior [J]. Journal of Intelligence, 2019, 38(10): 104-110.

[32] Public Solicitation of Opinions on the Interim Regulations on Management of Personal Information Protection in Mobile Internet Applications (Draft for Comment) [EB/OL]. [2021-04-26]. http://www.gov.cn/xinwen/2021-04/26/content_{5602780}.htm.

[33] People's Daily Online. Release of the Top Ten Initiatives for Personal Information Protection of Mobile Internet Application Users [EB/OL]. [2021-01-10]. http://it.people.com.cn/n1/2020/0110/c1009-31543883.html.

Author Contributions:
Zhou Yi: Topic selection and design, overall research framework design, paper revision;
Liu Yu: Research framework design, initial draft writing;
Nong Yanqing: Sample collection and data statistical analysis, participation in initial draft writing.

Note: Figure translations are in progress. See original paper for figures.