Postprint: An Evaluation Study of Personal Privacy Protection Policies on Chinese Government Open Data Platforms

Authors: Sun Ruiying, Li Jieru

Date: 2023-04-01T15:51:27+00:00

Abstract

[Purpose/Significance] To evaluate the personal privacy protection policies of China's government open data platforms and advance personal privacy protection on these platforms. [Method/Process] Based on the Personal Information Protection Law of the People's Republic of China and relevant literature, the Delphi method and Analytic Hierarchy Process were employed to construct an evaluation system, and the personal privacy protection policies of 16 provincial-level government open data platforms in China were analyzed, thereby completing the evaluation of personal privacy protection policies for China's government open data platforms. [Results/Conclusion] The personal privacy protection policies of China's government open data platforms are inadequately formulated and exhibit a generally low level of quality; it is necessary to strengthen supervision and improve personal privacy protection policies from multiple aspects, including policy implementation, protection awareness, and allocation of rights and responsibilities.

Full Text

Preamble

Title: Research on the Evaluation of Personal Privacy Protection Policies for Government Data Open Platforms in China

Authors: Sun Ruiying, Li Jieru
Affiliation: School of Information Management, Heilongjiang University, Harbin 150080

Abstract:
[Purpose/Significance] This study evaluates personal privacy protection policies for government data open platforms in China to advance privacy protection

on these platforms. [Method/Process] Based on the Personal Information Protection Law of the People's Republic of China and relevant literature, we constructed an evaluation system using the Delphi method and analytic hierarchy process, analyzing privacy protection policies across 16 provincial government data open platforms. [Result/Conclusion] The findings reveal that privacy protection policies on Chinese government data open platforms are inadequately implemented and generally low in quality, requiring strengthened supervision and improvement in policy implementation, protection awareness, and rights-responsibility allocation.

Keywords: Government data open platform; Personal privacy protection policy; Delphi method; Analytic hierarchy process
Classification Number: G250
DOI: 10.13266/j.issn.0252-3116.2022.12.001

In 2015, the State Council issued the *Outline for Promoting Big Data Development*, explicitly proposing the Digital China strategy to drive transformation in production, lifestyle, and governance through digitalization. Government data open platforms, led by government organizations, have assumed the responsibility of making publicly available information from various government departments accessible to the public [1]. Following the *Outline*, national policies and regulations related to data opening have grown rapidly [2]. In 2017, the state released *Several Opinions on Promoting the Opening of Public Information Resources*, and in 2018 issued the *Pilot Work Plan for Opening Public Information Resources*, leading to vigorous development in "building a unified national government data open platform and formulating public institution data opening plans" [3-4]. According to Fudan University's *China Local Government Data Open Report: Indicator System and Urban Benchmarks* released on July 26, 2021, by the end of April 2021, 174 provincial and municipal local governments in China had launched data open platforms, including 18 provincial platforms (including provinces and autonomous regions, excluding municipalities and Hong Kong, Macao, and Taiwan) and 156 city platforms (including municipalities, sub-provincial cities, and prefecture-level administrative regions) [5].

Government open data platforms provide convenience for public life and work, but simultaneously raise concerns about personal privacy, national security, and commercial confidentiality leaks, particularly frequent personal privacy breaches that damage citizens' interests [6]. To balance data openness with personal privacy protection, China began with the 2012 *National People's Congress Decision on Strengthening Network Information Protection*. In June 2017, the *Cybersecurity Law*, *E-commerce Law*, and *National Cyberspace Security Strategy* were enacted. Beyond specialized cyber laws, the *Consumer Rights Protection Law (Revised)* (2013), *Criminal Law Amendment (IX)* (2015), and *Civil Code (Personality Rights)* (2020) all supplemented personal information protection clauses, responding to public concerns. For example, the *General Principles of the Civil Law of the People's Republic of China* enacted on October 1, 2017 stipulated that "personal information of natural persons is protected by law, and

any organization or individual needing to obtain others' personal information shall obtain it legally and ensure information security," demonstrating national attention to cybersecurity and personal privacy.

On November 1, 2021, the *Personal Information Protection Law of the People's Republic of China* officially took effect, providing multi-scenario and multi-angle legal provisions based on different subjects for personal information protection issues, offering legal regulation and guidance for China's personal information protection work. As collectors, providers, and disseminators of basic data, government data open platforms are key to releasing data potential and a primary source of digital innovation [7]. The data resources provided by these platforms should exclude data otherwise stipulated by law or involving national interests, public security, commercial secrets, or personal privacy. However, in the freely open cyberspace, anyone can freely search, use, reuse, and redistribute data resources from government data open platforms, leading to occasional personal privacy leaks [8]. Therefore, these platforms must address personal privacy security issues, improve relevant policies and regulations, and ensure effective privacy protection.

2 Research Review and Logical Framework

2.1 Research Review

Research on privacy protection in government data opening abroad started earlier, but due to inconsistent privacy protection systems across countries, research perspectives are relatively scattered, focusing on: Personal privacy information disclosure concerns. M.J. Culnan [31] argued that such concerns primarily arise when individuals provide data to organizations without knowing how it will be used. Privacy information disclosure willingness. S.J. Milberg et al. [32] proposed that individuals' cognition and tolerance for privacy concession vary under different circumstances; M.J. Culnan et al. [33] believed individuals only have willingness to disclose when benefits equal or exceed risks; A. Beldad et al. [34] found that the sensitivity of personal data disclosed in e-government activities correlates with negative and positive risk perceptions; D.Q. Agozie [35] explored how privacy information transparency helps alleviate privacy fatigue in e-government. Factors influencing privacy data concerns. T. Zukowski et al. [36] believed concerns are mainly influenced by gender, age, and education; S. Youn [37] studied subjective factors like self-efficacy in information protection and privacy risk tolerance; Y.J. Park [38] examined external influences from culture, social environment, and legal regulation. Personal data protection surveys. Y. Wu [39] compared foundations, technical support, and practical verification for protecting personal data in the US, Germany, and China. Privacy protection technologies. H. Yun et al. [40] noted that in the big data era, collection, processing, and dissemination of personal privacy information have permeated all aspects of private life; A. Nikiforova [41] studied data intelligence technologies for the Society 5.0 era to empower government data opening; J.S. Lee et al. [42] proposed a method to integrate two or more de-identified govern-

ment open datasets to achieve appropriate balance between privacy disclosure risk and data utility.

Domestic research on privacy protection in government data opening mainly covers: Stakeholder relationships in government data opening. Zhu Xiaofeng et al. [16-17] analyzed behavioral characteristics and symbiotic mechanisms of stakeholders using the COVID-19 pandemic as an example. Privacy protection technologies. Yu Mengyue et al. [18] studied US government open data metadata standards; Zhou Linxing et al. [19] proposed technical governance methods from a privacy information governance perspective; Liu Donglan et al. [20] conducted data security analysis and anti-leakage technology research based on big data business scenarios; Wei Yinzhen et al. [21] studied blockchain and smart contract-based scientific data security traceability methods. Privacy risk control. Liu Jianxin et al. [22] studied a "dual-track system" for government data opening and sharing guarantees, constructing government data review rules; Chen Lanjie et al. [23] established a blockchain-based open government data personal privacy protection model. Foreign privacy protection policy and law analysis. Huang Ruhua et al. [24-25] analyzed privacy protection laws and policies in government data opening in the US and UK; Chen Mei et al. [26-27] studied privacy policies in the US, Brazil, South Korea, Spain, New Zealand, and Canada; Chu Jiewang et al. [28] reviewed US personal privacy protection policies in government open data practice. Balance between government data opening and privacy protection. Wu Yaguang [29] used the principle of proportionality to judge the limits of personal privacy information disclosure; Zhou Huan et al. [30] studied coordination and balance between data opening and privacy protection in practice.

Comprehensive research specifically matching government data open platform personal privacy protection policy evaluation is limited. Du Hehua [9-10] reviewed privacy policies of US, UK, and Australian government data open platforms, constructing an evaluation index system from three dimensions (government obligation notification, privacy security protection management, and personal rights protection), and evaluated Chinese platforms; Tong Linjie et al. [11] explored data security and privacy protection from an information ecology perspective; Wanyan Dengdeng et al. [12] conducted compliance reviews of user agreements on Chinese local government data open platforms; Ding Hongfa et al. [13] studied data security and privacy protection countermeasures based on data lifecycle theory; foreign scholars K. Patel [14] and L. Kristian [15] emphasized that governments should distinguish personal characteristic options in automated decision-making during data opening and avoid providing information covering all citizens.

Literature review reveals few papers on government data open platform privacy protection policy evaluation. Therefore, we expanded the scope to privacy protection research in government data opening to discover theoretical foundations. We found that while scholars have begun paying attention to personal privacy protection in government data opening, research remains limited and

fragmented without forming a complete system. Compliance governance based on legal provisions is particularly lacking. China's newly issued *Personal Information Protection Law* clarifies principles for personal information protection, providing the institutional foundation for collecting and using personal information and building specific protection rules [43]. Implementing this law and protecting personal information rights and security is the obligation and responsibility of government data open platforms. However, research based on the *Personal Information Protection Law* to evaluate domestic platform privacy protection policies is currently absent.

2.2 Analysis of Personal Privacy Issues in Government Data Open Platforms

2.2.1 Privacy Policy Settings on China's Provincial Government Data Open Platforms The *Personal Information Protection Law* contains specific provisions for personal information processing activities on government data open platforms. An investigation of existing provincial and municipal platforms from a privacy policy perspective revealed: Platforms have privacy policies that cannot be accessed. For example, Hubei's platform has a privacy policy that cannot be viewed. Platforms lack dedicated privacy policies. Such platforms are embedded in provincial government portals and use non-platform-specific privacy policies, including Jiangsu, Qinghai, and Hunan. Platforms have not yet established privacy policies, such as Chongqing and Xinjiang Uygur Autonomous Region.

2.2.2 Personal Privacy Protection Issues on Government Data Open Platforms The investigation found that even platforms with privacy policies have issues: Inadequate data review. As data collectors and publishers, platforms should review collected data for compliance and usability. However, Guangdong's platform disclaimer states: "The operation and management unit of 'Open Guangdong' only conducts formal review of various information published on the platform. The accuracy, completeness, legality, and authenticity of data information involved in public information resources on 'Open Guangdong' are subject to the relevant government departments or third-party institutions that register and publish the resources." This shows only formal review without unified standards, easily leading to privacy leaks. Personal information publication leaks. Platforms sometimes open citizens' ID numbers [25]. Insufficient data desensitization. Inadequate desensitization during collection, processing, storage, publication, and utilization creates privacy security vulnerabilities and assessment lags [44].

2.2.3 Necessity of Evaluating Platform Privacy Policies Privacy policies are essential for personal privacy protection on government data open platforms. However, investigation shows platforms either lack privacy protection policies or have policies that don't comply with the *Personal Information Protection Law* and fail to protect personal privacy. Therefore, an evaluation sys-

tem should be established to promote policy improvement and advance privacy protection work.

2.3 Research Framework

This study focuses on platform privacy protection policies, constructing an evaluation system and conducting empirical analysis:

(1) Use content analysis to analyze the seven chapters of the *Personal Information Protection Law* to establish influencing factors and analytical dimensions for evaluating government data open platform privacy protection policies.

(2) Use AHP with Yaahp 12.0 software to build a hierarchical model with target layer, criterion layer, sub-criterion layer, and indicator layer. Apply the Delphi method to invite experts to score indicator weights, then use Pareto classification to identify core, ordinary, and secondary indicators.

(3) Assign values to evaluation indicators to calculate platform scores and analyze results.

3 Evaluation of Privacy Policies for Government Data Open Platforms

3.1 Selection of Evaluation Dimensions and Indicators

Given economic and social complexity and diverse personal information processing scenarios, the *Personal Information Protection Law* stipulates specific circumstances for lawful personal information processing and provides targeted provisions for joint processing and entrusted processing. Government data opening must comply with the law while protecting personal information rights. Therefore, evaluation dimensions and indicators should be based on the *Personal Information Protection Law*, not exceeding the scope and limits necessary for legal duties, and establishing correspondence with the legal system to leverage its guiding and regulatory role [45]. The law text, with its strict review procedures and high lexical standards, provides ideal data for indicator selection [46].

Our indicator design is based on the *Personal Information Protection Law* enacted on November 1, 2021. The law comprises eight chapters; Chapter VIII (Supplementary Provisions) mainly contains term explanations and effective date and was excluded from indicator construction. We analyzed the remaining seven chapters using content analysis to establish three evaluation dimensions (Figure 2 [Figure 2: see original paper]).

We balanced external logic among chapters and internal logic among articles, refined legal provisions, reviewed relevant literature, and based on existing research [43], screened and organized the indicator system to construct a three-level system with 3 first-level indicators, 7 second-level indicators, and 20 third-

level indicators (Table 1). This system is grounded in China's newly issued personal information (privacy) protection law and national conditions, differing from previous studies that analyzed foreign laws and policies to guide Chinese platforms [47-48].

(1) **Personal Information Processing Rules (A)**: Refers to descriptions of various rules for processing personal information in privacy protection policies, with two sub-indicators: Routine Personal Information Disposal (A1) and Cross-border Personal Information Disposal (A2), based on Chapters II and III of the law.

Routine disposal describes notifications about personal information processing methods, storage methods, usage methods, sensitive personal information handling, and third-party entrustment. These indicators explain extraction and usage scenarios and describe information destinations, ensuring basic user information security. More detailed rule descriptions indicate more comprehensive personal information disposal [49].

Cross-border disposal describes notifications about cross-border provision and security assessment of personal information. For business-required cross-border processing, privacy policies should inform individuals of the recipient's name, contact information, processing purpose, etc., obtain separate consent, and conduct necessary security assessments. This indicator ensures information 出境 security and promotes cross-border information exchange.

(2) **Personal Rights Protection (B)**: Refers to descriptions and guarantees of personal rights in privacy protection policies, with two indicators: General Rights Protection (B1) and Special Rights Protection (B2), based on Chapter IV of the law.

General rights protection describes notifications about rights to information access, modification, restriction of processing, and erasure ("right to be forgotten"). China's personal information protection ultimately focuses on individual rights, building a rights system centered on individual "informed consent" and safeguarded by query, correction, and deletion rights [50]. Protecting basic personal information rights is the cornerstone of protection construction.

Special rights protection describes notifications about minors' privacy rights and rights protection after natural death. As online information publishers and users, minors' information rights require balancing protection with freedom of expression. Regulations like the *Regulations on the Protection of Children's Personal Information Online* provide safety protection for minors' online activities [51], and their information should also be protected on government data open platforms according to law. Protection of information after natural death should also be addressed.

(3) **Personal Information Processor Obligations (C)**: Refers to descriptions of obligations that information processors should undertake, with three indicators: Personal Information Protection Measures Setting (C1),

Personal Information Processing Flow Guarantee (C2), and Complaint Feedback Channels (C3), based on Chapters V, VI, and VII.

Protection measures setting describes technical and institutional guarantees mentioned in privacy policies. Institutional guarantee refers to management systems with clear rights and responsibilities, while technical measures involve de-identification, encrypted storage, and computing technologies [52]. National policies like the *Cybersecurity Law*, *Civil Code*, and *Personal Information Protection Law* provide references for management system formulation.

Processing flow guarantee describes pre-use assessment and post-incident remedy plans. Privacy protection should be full-process, covering not only rights notification during use but also pre-use security assessment and emergency plans for special circumstances.

Complaint feedback channels describe where, how, and when users can get responses. During government data opening, platforms should provide channels and processing rules to promote sustainable development.

3.2 Evaluation Indicator Validity Assessment

Although based on authoritative legal texts, the indicator system's scientific validity requires verification. We used the Delphi method, distributing questionnaires to 10 experts in government open data platforms. Using a Likert scale, experts rated indicator importance across five levels. We calculated indicator membership degree to measure relationships, where higher values indicate greater influence on platform privacy protection policy evaluation.

The membership degree formula is:
$(P1 + 0.75\times P2 + 0.5\times P3 + 0.25\times P4 + 0\times P5) / (P1 + P2 + P3 + P4 + P5)$

Where P1-P5 represent counts of experts rating the indicator as very important to very unimportant, with weights 1, 0.75, 0.5, 0.25, 0 respectively.

Calculated membership degrees are shown in Table 2 . Values below 0.7 indicate insufficient validity and should be removed [53]. All indicators in this study exceed 0.7, requiring no removal. Values between 0.7-0.79 indicate basic validity (e.g., first-level indicator C, second-level indicators B1 and C3, third-level indicators A11, A12). Values between 0.8-0.89 indicate strong validity (e.g., first-level indicator A, second-level indicator C1, third-level indicator B12). Values between 0.9-0.99 indicate very high validity (e.g., first-level indicator B, second-level indicator B2, third-level indicator A14). Overall, indicators demonstrate good validity for evaluation.

3.3 AHP-Based Evaluation System Construction

The Analytic Hierarchy Process, proposed by Thomas L. Saaty in the 1970s, is suitable for complex, multi-criteria decision problems [54]. Given the numerous

and dispersed privacy policy provisions involving different personnel responsibilities and scenarios, AHP can decompose policies into target, criterion, and indicator layers to reasonably set weights and comprehensively reflect content for quantitative and qualitative evaluation.

Following AHP principles: First, the Delphi method was used to construct pairwise comparison matrices with 1-9 scales, distributed to 10 domain experts. Using Yaahp software, we built a hierarchical model and calculated the geometric mean of expert scores. The maximum eigenvalue (MAX) and eigenvector (W) were solved, with eigenvector values representing indicator weights. After consistency verification, results are shown in Table 3 .

We applied Pareto analysis (primary-secondary factor analysis) to identify core indicators. Traditional 0-80%, 80%-90%, 90%-100% classifications are not conducive to identifying core indicators and may overemphasize less influential ones. Therefore, we narrowed the cumulative weight range for core indicators [55]. Since core indicators play decisive roles, their cumulative weight maximum should exceed 50% (i.e., >0.5 of total weight 1). We determined the reasonable interval as [0, 0.6]. Table 4 shows indicators sorted by weight with cumulative weights, establishing core indicators A (0-0.6), ordinary indicators B (0.6-0.9), and secondary indicators C (0.9-1).

Analysis shows 7 core indicators are primary factors, especially important. Seven ordinary indicators, while not decisive, significantly influence quality improvement. Six secondary indicators, though less critical, still directly or indirectly affect protection and require attention.

4 Empirical Evaluation of Platform Privacy Protection Policies

4.1 Sample Selection

Based on Fudan University's *China Local Government Data Open Report* [5], we selected samples meeting: Officially authorized government data open platforms; Provincial or municipality-level representation; "Centralized proprietary" form (independent platforms, not embedded in government portals); Containing privacy-related texts like user agreements or legal statements. From 22 provincial platforms (surveyed October 24-30, 2021), we excluded inaccessible samples (Hubei), "centralized embedded" platforms (Jiangsu, Qinghai, Hunan), and platforms without privacy policies (Chongqing, Xinjiang). The final sample comprised 16 platforms (13 provinces, 3 municipalities), shown in Table 5 .

4.2 Scoring Method

Using web investigation and content analysis, we examined each platform's privacy protection policy. Adopting weighted scoring from Wanyan Dengdeng [12], we assigned 1 point for compliance with third-level indicators (Hi = 1) and 0 for non-compliance (Hi = 0), with no intermediate values. Let Ci be the weight of

indicator i; the actual score is Ti = Ci Hi. The platform's total score (converted to percentage) is T = Ci Hi 100, where $1 \leq n \leq 20$, n is integer.

4.3 Results Analysis

The 16 platforms averaged only 29.64 points, reflecting inadequate or missing privacy protection policy texts. Platforms lack norms and supervision in information collection, use, processing, and protection, risking privacy leaks and undermining public trust. Scores show polarization: Guizhou (55.21) and Sichuan (55.21) performed well with independent privacy statements covering all core indicators, including top-ranked Personal Information Use Method Notification (A13, weight 0.1074) and fourth-ranked Personal Information Processing Method Notification (A11, weight 0.0879) (Figure 3 [Figure 3: see original paper]).

Most platforms mention privacy protection in website statements or disclaimers rather than dedicated policies. Hebei's platform (score 0), launched recently, lacks privacy protection provisions entirely (Figure 4 [Figure 4: see original paper]), showing significant gaps despite high data openness.

(1) Analysis of "Personal Information Processing Rules—Indicator A" (Figure 5 [Figure 5: see original paper]). Investigation found existing provisions unclear. No platforms addressed cross-border disposal (A2) or sensitive personal information handling notification (A14). Among core indicators, only 5 of 16 platforms covered top-ranked personal information use method notification (A13), and only 7 covered fourth-ranked processing method notification (A11). Only 3 covered sixth-ranked storage method notification (A12). For ordinary and secondary indicators like sensitive information description (A14), almost no provincial platforms provided content. While most platforms promised not to provide, sell, rent, share, or trade personal information to third parties, they failed to specify applicable scenarios or corresponding safeguards/remedies (Figure 6 [Figure 6: see original paper]).

(2) Analysis of "Personal Rights Protection—Indicator B" (Figure 7 [Figure 7: see original paper]). Only information access rights (B11, second in importance) were well-implemented (15/16). Other rights like modification (B12, 1/16), restriction (B13, 1/16), and erasure (B14, 1/16) were poorly implemented. No platforms addressed minors' privacy protection (B21) or post-mortem rights protection (B22). Minors' privacy protection (B13) and restriction of processing rights (B13) rank third and fifth in importance, respectively, yet their absence indicates weak rights protection awareness requiring multi-faceted improvement.

(3) Analysis of "Personal Information Processor Obligations—Indicator C" (Figure 8 [Figure 8: see original paper]). Only 7 provincial platforms promised technical safeguards (C11, seventh in importance), lacking specific technical descriptions. Institutional guarantees (C12) were better, with 11 provinces mentioning legal compliance. Pre-assessment (C21) and

post-remedy (C22) measures need improvement: 11 platforms mentioned pre-publication review, and 10 established post-incident remedies but without specific measures and with disclaimers of responsibility. Critically, no platforms established complaint application methods (C32) or feedback time limits (C33), though all had disclaimers, showing strong risk avoidance tendencies (Figure 9 [Figure 9: see original paper]).

5 Strengthening Personal Privacy Protection on Government Data Open Platforms

5.1 Awareness

The *Personal Information Protection Law* (Article 57) requires government data open platforms, as basic internet service providers with massive users and complex business types, to supervise personal information processing activities, stop services for serious violators, publish social responsibility reports, and accept public supervision. As public authorities, platforms only control (not decide) personal information collection and must strictly limit surveillance technologies and facial recognition in public spaces [56]. Platforms should provide necessary information literacy education, inform users of risks and safeguards, and offer choices. However, only 7 platforms addressed personal information processing method notification (A11) and only 3 addressed storage method notification (A12), while sensitive information handling (A14) was absent. Platforms must raise privacy protection awareness and establish safeguards and remedies.

5.2 Adjustment

Platforms show deficiencies in technical and institutional descriptions, lack complaint channels, and exhibit strong risk avoidance. Only 7 platforms promised technical safeguards, institutional management needs improvement, pre-assessment and post-remedy measures require enhancement, and no platforms established complaint methods or feedback time limits. Platforms need privacy protection training and clear management policies: First, establish unified national privacy protection management standards based on individual "consent" principles, prohibiting misleading, fraudulent, or coercive consent acquisition. Second, platforms cannot refuse services for "non-consent" or "consent withdrawal." Third, image collection and personal identification devices in public spaces must be strictly limited to public safety purposes with clear signage. Fourth, automated decision-making, information push, or commercial marketing must provide non-personalized alternatives or convenient refusal methods for sensitive information like biometrics, financial accounts, location tracking, and medical health.

5.3 Alignment

With multiple platforms providing vast public data resources, optimized combination requires partnership and collaboration to identify inconsistencies, in-

accuracies, or incompleteness. Beyond guaranteeing information access rights, platforms must strengthen implementation of modification rights (B12), restriction rights (B13), erasure rights (B14), and supplement minors' privacy protection (B21) and post-mortem rights protection (B22) to calibrate personal information resources across systems. First, platforms should proactively delete personal information when purposes are achieved, services stop, or retention periods expire. Second, when discovering violations, platforms should remind and delete information. Third, platforms should correct, supplement, or delete data according to other laws and regulations.

5.4 Assistance

No provincial platforms established complaint application methods (C32) or feedback time limits (C33), though all have disclaimers, indicating citizens cannot obtain effective help when privacy rights are violated. First, platforms should clarify and inform users of their information rights and corresponding operation methods, promising protection forms. Second, platforms should provide more effective and complete records connecting users with platform resources for better assistance when privacy is violated. Third, platforms should conspicuously, clearly, and completely inform processors' names/contact information, processing purposes/methods, information types/retention periods, individual rights and exercise procedures, and other legally required matters to ensure transparent and fair decision-making.

5.5 Advocacy

Government data open platforms' primary responsibility is providing secure and convenient information services, promoting data resource recreation and deployment, strengthening interoperability, improving execution, and better integrating resources to meet citizen and societal needs. To improve the public data resource system (excluding data involving national interests, public security, commercial secrets, or personal privacy), strengthen public data governance, enhance sharing efficiency, and expand orderly opening, we must advocate building a unified and balanced public data operation mechanism that integrates data opening with privacy protection. This requires establishing specialized government data opening privacy protection agencies or departments to formulate new policies ensuring smooth privacy protection implementation.

References

[1] Huang Ruhua, Wang Chunying. Investigation and Analysis of Government Data Open Platforms in China[J]. Information Studies: Theory & Application, 2016, 39(7): 50-55.
[2] Huang Ruhua, Wen Fangfang. Policy Framework and Content of Government Data Opening and Sharing in China: Content Analysis of National Policy Texts[J]. Library and Information Service, 2017, 61(20): 12-25. DOI:

10.13266/j.issn.0252-3116.2017.20.002.
[3] State Council. Notice on Issuing the Outline for Promoting Big Data Development[EB/OL]. [2022-03-31]. http://www.scio.gov.cn/xwfbh/xwbfbh/wqfbh/33978/34896/xgzc34902/Documer
[4] Chen Chuanfu, Deng Zhiqing. Research on Improving the Subject System of Government Data Opening[J]. Information Science, 2019, 37(1): 3-8, 21.
[5] Fudan University Digital & Mobile Governance Lab. China Local Government Data Open Report (First Half of 2021)[EB/OL]. [2021-07-26]. http://www.dmg.fudan.edu.cn.
[6] Zhang Jiale, Zhao Yanchao, Chen Bing, et al. Research on Data Security and Privacy Protection in Edge Computing[J]. Journal on Communications, 2018, 39(3): 1-21.
[7] Zhu Yongwei. Research on Data Opening and Sharing Between Industrial Internet Platforms[J]. China Informationization, 2019(11): 87-89.
[8] Zhang Maoyue. Risks and Responses for Citizens' Personal Information Data in the Big Data Era[J]. Library Development, 2020(3): 67-75.
[9] Du Hehua. Research on Constructing a Privacy Protection Evaluation System for Government Data Open Platforms in China[J]. Information Science, 2021(11): 157-166.
[10] Du Hehua. Investigation and Reference of Foreign Government Data Open Platform Privacy Protection Policies[J]. Information Studies: Theory & Application, 2015, 38(6): 57-61, 70.
[11] Tong Linjie, Liu Bo. Research on Data Security and Privacy Protection in Government Data Opening from an Information Ecology Perspective[J]. Library Theory and Practice, 2020(5): 67-72.
[12] Wanyan Dengdeng, Tao Chengxu. Compliance Assessment of User Agreements on Government Data Open Platforms[J]. Library Tribune, 2021, 41(7): 116-124.
[13] Ding Hongfa, Meng Qiuqing, Wang Xiang, et al. Analysis of Data Security and Privacy Protection Countermeasures for Government Data Opening Oriented to Data Lifecycle[J]. Journal of Intelligence, 2019, 38(7): 151-159.
[14] Patel K, Jethava GB. Privacy Preserving Techniques for Big Data: A Survey[C]//Proceedings of 2018 2nd International Conference on Inventive Communication and Computational Technologies. Coimbatore, 2018: 194-199.
[15] Larsson KK. Digitization or Equality: When Government Automation Covers Some, but Not All Citizens[J]. Government Information Quarterly, 2021, 38(1): 1-10.
[16] Zhu Xiaofeng, Sheng Tianqi, Zhang Wei. Research on Symbiotic Operation Mechanism of Government Data Opening Under Major Public Health Emergencies: Construction and Evolution[J]. Information Studies: Theory & Application, 2020, 43(12): 80-88.
[17] Zhu Xiaofeng, Sheng Tianqi, Cheng Lin. Evaluation Framework and Effectiveness Research on Government Data Open Platforms from a Service Contact Perspective[J]. E-Government, 2021(10): 2-14.
[18] Yu Mengyue, Zhai Jun, Lin Yan, et al. Metadata Standards for US Government Open Data and Their Implications: From a Catalog Aggregation Perspective[J]. Journal of Intelligence, 2017, 36(12): 145-151.

[19] Zhou Linxing, Zhou Li. Research on Privacy Information Governance in Government Data Opening[J]. Library Science Research, 2019(12): 41-47.
[20] Liu Donglan, Liu Xin, Zhang Hao, et al. Research on Data Security Analysis and Anti-Leakage Technology Based on Big Data Business Scenarios[J]. Shandong Electric Power Technology, 2020, 47(9): 7-13.
[21] Wei Yinzhen, Deng Zhonghua, Guan Yurong, et al. A Scientific Data Security Traceability Method Based on Blockchain and Smart Contracts[J]. Modern Information Technology, 2021, 41(1): 32-38.
[22] Liu Jianxin, Xu Huanran. Research on Guarantee Mechanisms for Government Data Opening and Sharing in China: Status, Problems, and Countermeasures[J]. Electronics Intellectual Property, 2021(4): 65-77.
[23] Chen Lanjie, Wen Hang. Research on Blockchain-Based Personal Privacy Protection Model and Implementation Mechanism for Open Government Data[J]. Library Theory and Practice, 2021(1): 67-72.
[24] Huang Ruhua, Liu Long. Research on Personal Privacy Protection in UK Government Data Opening[J]. Library Development, 2016(12): 47-52.
[25] Huang Ruhua, Li Nan. Research on Personal Privacy Protection in US Open Government Data[J]. Library, 2017(6): 19-24, 76.
[26] Chen Mei, Tan Weidong. Privacy Risk Assessment and Prevention in Government Open Data: New Zealand's Experience[J]. Information Studies: Theory & Application, 2020, 43(5): 110-114, 90.
[27] Chen Mei. Privacy Risk Control in Open Government Data: US Experience and Implications[J]. Journal of Intelligence, 2021, 40(8): 81-86.
[28] Chu Jiewang, Ding Hui. US Government Open Data Personal Privacy Protection Policy and Its Implications for China: Content Analysis of 52 Policy Texts[J]. Library and Information Service, 2021, 65(8): 140-150.
[29] Wu Yaguang. Public Limits of Personal Privacy Information in Government Data Opening[J]. Library Science Research, 2020(22): 45-52.
[30] Zhou Huan, Xing Qiangguo, Tang Yong. Research on Policy Synergy Between Data Opening and Privacy Protection Based on Policy Text Computation[J]. Library Tribune, 2021, 41(11): 118-127.
[31] Culnan MJ, Armstrong PK. Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation[J]. Organization Science, 1999, 10(1): 104-115.
[32] Milberg SJ, Smith HJ, Burke SJ. Information Privacy: Corporate Management and National Regulation[J]. Organization Science, 2000, 11(1): 35-57.
[33] Culnan MJ, Armstrong PK. Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation[J]. Organization Science, 1999, 1(10): 104-115.
[34] Beldad A, Md Jong, Steehouder M. I Trust Not Therefore It Must Be Risky: Determinants of the Perceived Risks of Disclosing Personal Data for E-Government Transactions[J]. Computers in Human Behavior, 2011, 27(6): 2233-2242.
[35] Agozie DQ. Discerning the Effect of Privacy Information Transparency on Privacy Fatigue in E-Government[J]. Government Information Quarterly, 2021, 38(4): 101601.

[36] Zukowski T, Brown I. Examining the Influence of Demographic Factors on Internet Users' Information Privacy Concerns[C]//Proceedings of the 2007 Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists on IT Research in Developing Countries. ACM, 2007: 197-204.
[37] Youn S. Determinants of Online Privacy Concern and Its Influence on Privacy Protection Behaviors Among Young Adolescents[J]. The Journal of Consumer Affairs, 2009, 43(3): 389-418.
[38] Park YJ. Digital Literacy and Privacy Behavior Online[J]. Communication Research, 2013, 40(2): 215-236.
[39] Wu Y. Protecting Personal Data in E-Government: A Cross-Country Study[J]. Government Information Quarterly, 2014, 31(1): 150-159.
[40] Yun H, Lee G, Kim DJ. A Chronological Review of Empirical Research on Personal Information Privacy Concerns: An Analysis of Contexts and Research Constructs[J]. Information & Management, 2019, 56(4): 570-601.
[41] Nikiforova A. Smarter Open Government Data for Society 5.0: Are Your Open Data Smart Enough?[EB/OL]. [2021-08-29]. https://doi.org/10.3390/s21155204.
[42] Lee JS, Jun SP. Privacy-Preserving Data Mining for Open Government Data from Heterogeneous Sources[J]. Government Information Quarterly, 2021, 38(1): 101544.
[43] Sun Ruiying, Li Jieru. Research on the Current Status of Personal Information Protection Work in China: Interpretation Based on the Draft of the Personal Information Protection Law of the People's Republic of China (Second Draft)[J]. Information Science, 2021(11): 157-166.
[44] Wu Zhongcan. Privacy Risks in Government Data Opening: Types, Causes, and Governance Strategies[J]. Journal of Guizhou Provincial Party School, 2021(5): 38-48.
[45] Zhang Demiao, Li Chao. The Generation and Evolution Logic of China's Rule of Law Evaluation Indicator System: A Processual Explanation from Rule of Law Concept to Evaluation Indicators[J]. Theory and Reform, 2015(2): 126-133.
[46] Rossi PH, Lipsey MW, Freeman HE. Evaluation: A Systematic Approach[M]. Translated by Qiu Zeqi, Wang Xuhui, Liu Yue, et al. 7th ed. Chongqing: Chongqing University Press, 2007: 49.
[47] Chen Mei, Liang Yikai. Canada's Privacy Impact Assessment Policy: History, Content, Analysis, and Implications[J]. Library and Information Service, 2021, 65(17): 142-151.
[48] Chen Mei. Research on Privacy Risk Control in Korean Open Government Data[J]. Information Studies: Theory & Application, 2021, 44(8): 180-186, 111.
[49] Cui Congcong. Institutional Construction of Personal Information Restriction Processing Rights: Amendment Suggestions for Article 44 of the Personal Information Protection Law (Draft)[J]. Exploration and Free Views, 2020(11): 24-33.
[50] Zhang Jin. Personal Information Protection: Beyond the Limitations of Individual Rights Thinking[J]. Journal of Dalian University of Technology (Social Sciences Edition), 2021, 42(1): 90-97.

[51] Sun Yu, Luo Weilin. From Personal Data Protection to Data Subject Personality Rights Protection: Comments on the Implementation of the Regulations on the Protection of Children's Personal Information Online[J]. E-Government, 2020(12): 52-58.
[52] Shang Xixue, Han Haiting. Research on Personal Information Protection Paths in Government Data Opening[J]. E-Government, 2021(6): 113-124.
[53] Sun Ruiying, Ma Xiaowei. Evaluation of Think Tank Service Capabilities of University Libraries[J]. Library Tribune, 2021, 41(8): 120-131.
[54] Huang Yue, Zhou Lixia, Pu Pan. Research on Optimization Decision-Making of China's Information Security Policy Based on AHP Method[J]. Modern Information Technology, 2015, 35(3): 77-81.
[55] Qu Zhikai, Zhang Qiubo, Lan Yuexin, et al. Research on Network Public Opinion Risk Early Warning for Terrorist Violence Events[J]. Journal of Intelligence, 2016, 35(6): 40-46.
[56] Liu Shiguo. Jurisprudence of Information Control Rights and China's Personal Information Protection Legislation[J]. Political Science and Law Review, 2021, 4(3): 80-91.

Author Contributions:
Sun Ruiying: Responsible for conceptualizing viewpoints, framework design, writing and revision;
Li Jieru: Responsible for data collection, data analysis, and paper writing.

Research on the Evaluation of Personal Privacy Protection Policies of Government Data Open Platforms in China

Sun Ruiying, Li Jieru
School of Information Management, Heilongjiang University, Harbin 150080

Abstract:
[Purpose/Significance] Evaluate the personal privacy protection policies of government data open platforms in China to promote personal privacy protection on these platforms. [Method/Process] Based on the Personal Information Protection Law of the People's Republic of China and related literature, this study uses the Delphi method and analytic hierarchy process to construct an evaluation system, analyzing the personal privacy protection policies of 16 provincial government data open platforms in China to complete the evaluation. [Result/Conclusion] The personal privacy protection policies of government data open platforms in China are inadequately implemented, with an overall low level. It is necessary to strengthen supervision and improvement of personal privacy protection policies from multiple aspects including policy implementation, protection awareness, and rights-responsibility allocation.

Keywords: Government data open platform; Personal privacy protection policy; Delphi method; Analytic hierarchy process

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