Algorithmic Peering and Privacy Protection: Exploring the Influencing Factors and Paths of User Privacy Boundaries in Library Intelligent Services*

Jia Ruonan Su Qiya

2026-07-24

ChinaRxiv

Abstract

Exploring the factors influencing users' privacy boundaries in library intelligent services in the digital-intelligent era helps protect users' privacy rights and interests and improve the quality of intelligent services. Drawing on communication privacy management theory, this study constructs a conceptual model and uses fuzzy-set qualitative comparative analysis to conduct a configurational analysis of the factors influencing users' privacy boundaries in library intelligent services. The findings show that users' privacy boundaries are jointly shaped by multiple factors, including privacy value orientation, perceived privacy risk, perceived privacy control, algorithm appreciation, algorithm aversion, algorithmic hegemony, and privacy policies. Among them, perceived privacy control is a key variable affecting users' privacy boundaries in library intelligent services; the privacy boundary management strategies of users of library intelligent services exhibit diversified characteristics.

Full Text

【Users ·Services】

Algorithmic Peering and Privacy Protection:

Exploring the Influencing Factors and Paths of User Privacy Boundaries in Library Intelligent Services*

Jia Ruonan Su Qiya
School of Public Administration, Xiangtan University, Xiangtan 411105

Abstract Exploring the factors influencing users' privacy boundaries in library intelligent services in the digital-intelligent era can help safeguard users' privacy rights and interests and improve the quality of intelligent services. Drawing on communication privacy management theory, this study constructs a conceptual model and uses fuzzy-set qualitative comparative analysis to conduct a configurational analysis of the factors affecting users' privacy boundaries in library intelligent services. The study finds that users' privacy boundaries are jointly shaped by multiple factors, including privacy value orientation, perceived privacy risk, perceived privacy control, algorithm appreciation, algorithm aversion, algorithmic hegemony, and privacy policies. Among these, perceived privacy control is a key variable influencing users' privacy boundaries in library intelligent services; strategies for managing users' privacy boundaries in library intelligent services exhibit diversified characteristics.

[**Keywords**] library intelligent services; communication privacy management theory; privacy boundary

[**CLC Classification No.**] G250.7; G252 [**Document Code**] A [**Article No.**] 1003-7845(2026)03-0052-10

[**Citation Format**] Jia Ruonan, Su Qiya. Algorithmic Peering and Privacy Protection: Exploring the Influencing Factors and Paths of User Privacy Boundaries in Library Intelligent Services[J]. *Library Work in Colleges and Universities*, 2026(3): 52-61.

Introduction

With the full arrival of the digital-intelligent era, artificial intelligence is developing vigorously. Most libraries have formulated or are implementing artificial-intelligence-related plans to support the fulfillment of the library mission[1] and to continue advancing toward more intelligent and smarter libraries. Library intelligent services represent an organic integration in which information technology injects new concepts into traditional library services[2]. Centered on technologies such as artificial intelligence and the Internet of Things, and relying on intelligent platforms to provide digital services, they uphold a user-centered philosophy, create convenient and personalized innovative services, and improve the efficiency of library operation and management as well as the utilization rate of resources.

However, as information interaction continues to deepen, issues related to user privacy have become increasingly prominent. The *IFLA Trend Report 2024* points out that, as an important resource for the development of smart libraries, users' private information promotes service innovation while also facing severe challenges[3]. In the digital-intelligent era, when providing services to users, libraries need to collect, store, process, transmit, and otherwise handle users'information, involving identity information, borrowing records, access logs, reading preferences, and other content. If identity identifiers, sensitive private information, and other contents contained in user information cannot be properly protected, privacy security problems can easily arise, thereby affecting the construction and development of libraries. Therefore, under the model of library intelligent services, how users dynamically coordinate privacy boundaries and balance service needs with the protection of personal privacy has become an issue that urgently requires in-depth research and resolution.

At present, research on library intelligent services mainly focuses on two major aspects. First is the application of intelligent algorithms in library resource management and information services[4]. At the level of resource management, algorithms such as machine learning[5] and data mining[6] are applied to collection acquisition forecasting, decisions on weeding outdated books, dynamic resource allocation, and automatic classification and indexing, optimizing collection structures through the analysis of reader behavior and resource usage data. At the level of information services, technologies such as natural language processing[7], knowledge graphs[8], and optical character recognition[9] are widely applied in intelligent reference robots, intelligent document parsing,

in-depth knowledge recommendation, and digitized retrieval of library collections, so as to achieve precise delivery and efficient use of personalized content. Second are privacy and security issues. Research focuses on governance measures for user privacy information leakage; existing work discusses such issues from perspectives including identifying privacy risks[10], improving privacy policy systems[11], and cultivating readers' literacy in autonomous management of private information[12], thereby providing theoretical support and practical pathways for the sustainable development of libraries.

Although algorithm application and privacy protection have received extensive attention in the library field, the dynamic game structure between the two remains insufficiently revealed. Improvements in the effectiveness of library intelligent services are often accompanied by dynamic changes in users' privacy boundaries, while existing studies either emphasize technological optimization paths or remain at the level of single-factor privacy countermeasures, lacking a systematic deconstruction of the factors influencing privacy boundaries and empirical examination of their synergistic paths. In view of this, this study proceeds on the basis of existing research findings,

---

* This article is one of the research outcomes of the general project of Xiangtan University' s professional-degree postgraduate education and teaching reform research, "Analysis of Postgraduate Digital Literacy Education Needs and Curriculum Optimization from the Perspective of the Research Life Cycle" (Project No.: YJGYB202313).

Author Bio: Jia Ruonan, Ph.D., lecturer, master' s supervisor; research interests include online public opinion, user information behavior, and knowledge graphs. Su Qiya, undergraduate student; research interest: user information behavior.

Date Received: 2025-12-30 **Responsible Editor:** Jia Nan

attempts to address the following three questions: (1) What factors influence the privacy boundaries of users of library intelligent services? (2) What different configurational paths exist among these influencing factors? (3) What measures can be taken to improve the quality of library intelligent services while safeguarding user privacy?

1 Theoretical Foundations and Related Concepts

1.1 Communication Privacy Management Theory

Communication Privacy Management (CPM) theory was proposed by the American communication scholar S. Petronio[13] in *Boundaries of Privacy*, published in 2002. Its core view is that individuals control the dissemination of private information by constructing privacy boundaries and formulating boundary-management rules. Centered on multiple dimensions such as privacy-information management, the demarcation of privacy boundaries,

privacy-control strategies, and the construction of protection mechanisms, this theory clarifies the relationship between personal information and privacy, and explains the negotiation process through which individuals disclose private information[14]: first, an individual' s awareness of ownership over private information reflects that individual' s privacy value orientation, which directly affects their attitude toward and handling of private information. Second, perceived privacy risk and perceived privacy control are also key factors influencing individual privacy-management behavior. An individual' s perception of the adverse consequences that may result from privacy leakage affects the way they adopt privacy-protection measures; and their belief in their own ability to control personal private information affects how they disclose and manage private information. Once private information has been disclosed, the owner and the recipient of the information jointly assume corresponding management responsibilities. For this reason, many organizations formulate privacy policies that clarify the rules for the collection, use, storage, and sharing of personal information. Finally, individuals all have their own privacy boundaries and manage them according to certain rules; these rules are influenced by individuals' subjective cognition and are also continuously adjusted in the course of interpersonal interaction.

Compared with traditional privacy research, CPM theory breaks through the conventional perspective of "privacy as one-way protection." It places privacy behavior within the interactive context of interpersonal communication for analysis, emphasizing the permeability of privacy boundaries and the negotiability of management rules. The theory focuses not only on the role of individuals' subjective cognition, but also on the influence of the relationship between interacting parties and contextual factors, thereby providing an operable analytical framework for analyzing privacy behavior in diverse communication scenarios. At present, this theory has been extended to research on privacy issues in the field of information systems and can effectively reveal the mechanisms of users' privacy-information disclosure behavior. Its theoretical perspective and analytical logic are likewise applicable to library intelligent-service scenarios, and can provide theoretical support for understanding users' privacy-boundary issues in library intelligent services.

1.2 Privacy Boundaries of Users of Library Intelligent Services

A "boundary"is characterized by separation, implying a clear line of demarcation. CPM theory compares privacy to an elastic boundary extending from the self to others[13], emphasizing that it is a product of dynamic negotiation between users and the external environment rather than a static individual attribute. Therefore, privacy boundaries refer to the scope or limits within which private information can be controlled. In essence, they are virtual control boundaries constructed by individuals in the interaction of information dissemination, based on their cognition of ownership over private information and their own privacy value orientations, in order to distinguish private information from non-private

information and to define the dissemination scope and access permissions of private information. They are both the core vehicle through which individuals implement privacy-boundary management behaviors and an important mechanism for realizing privacy protection and information management. To manage privacy boundaries effectively, users establish a series of rules, and the opening or closing of privacy boundaries determines the flow state of information: when a boundary is open, information can flow freely; when a boundary is closed, the flow of information is restricted. Specifically, boundary permeability rules determine the amount, scope, and degree of disclosure of users' private information; boundary linkage rules clarify who may come into contact with users' privacy; and boundary ownership rules control the direction in which users' privacy is disseminated.

CPM theory holds that individuals interact with the external environment and protect private information by managing privacy boundaries[13]. This compromise and contestation over service needs is consistent with the management of users' privacy boundaries in library intelligent services. In library intelligent services, the connotation of privacy boundaries becomes further concretized: it refers to the rights boundaries that users establish, based on their own information rights and interests, with regard to information collection, storage, processing, use, and other behaviors throughout the entire process of intelligent services. The demarcation, adjustment, and maintenance of these boundaries are precisely the core negotiation process between users and libraries around rules for managing private information, and they are also the key research object of user privacy protection in this scenario. This provides new ideas for research on the privacy of users of library intelligent services.

2 Variable Selection and Model Construction

2.1 User Dimension

According to CPM theory, individuals' privacy value orientations are diverse, which in turn leads to significant differences in their behavioral decisions regarding information disclosure. In addition, perceived privacy risk and perceived privacy control profoundly influence how users define, protect, and manage their privacy boundaries in digital environments[15]. On this basis, this study selects three variables—privacy value orientation, perceived privacy risk, and perceived privacy control—as antecedent conditions in the user dimension.

Privacy value orientation is an individual' s general tendency to protect or restrict the disclosure of private information[16]. CPM theory holds that because individuals differ in their privacy value orientations, they often exhibit different needs for privacy-boundary management[17]. For example, users who pay greater attention to their own privacy will, when using library intelligent services such as precise recommendation and personalized retrieval, be more concerned about the risk that private information such as borrowing records and reading preferences may be misused or leaked. They will also be more cautious when handling

private information, and will usually choose to narrow the privacy boundaries in library intelligent services so as to protect their private information from infringement.

Perceived privacy risk is the expectation of losses associated with the disclosure of private information, representing a kind of uncertainty caused by potential negative consequences[15]. Perceived privacy risk not only affects the formation of privacy boundaries, but also

will have a significant impact on privacy-disclosure behavior[18]. CPM theory holds that, when deciding whether to open their privacy boundaries, individuals fully assess the potential risks of disclosing private information. The perceived level of privacy risk directly determines the strictness of the measures users adopt in managing their privacy boundaries. When users perceive privacy risks in library intelligent-service processes such as intelligent search, personalized recommendation, and data retention, they will proactively strengthen their awareness of privacy protection, give priority to guarding or narrowing their privacy boundaries, and prevent the risk of privacy leakage by turning off personalized services, hiding personal borrowing information, and taking similar actions.

Perceived privacy control is an individual' s subjective judgment of the extent to which they can control their own private information[19], and it has a significant impact on privacy-disclosure behavior. CPM theory holds that the formation of privacy boundaries depends to a large extent on users' belief that "the personal information they disclose can be reasonably collected and properly used" ; this belief is users' perceived privacy control[19]. When individuals have a relatively high level of perceived privacy control, their concerns about improper use of information are reduced, and they are therefore more willing to expand the openness of their privacy boundaries. In the context of library intelligent services, users with relatively high perceived privacy control will believe that they have autonomous operational authority over privacy settings, data viewing, and deletion in library intelligent services, and will thus judge the private information they submit in intelligent services to be relatively secure, making them more inclined to actively expand their privacy boundaries.

2.2 Algorithm Dimension

According to CPM theory, contextual factors affect users' privacy boundaries. In library intelligent services, special attention needs to be paid to the interactive relationship between algorithms and user privacy. Algorithm attitudes are generally divided into algorithm appreciation and algorithm aversion. They not only directly drive user behavior, but also profoundly influence social relationships and the direction of algorithmic development. In addition, existing studies have pointed out that algorithmic fairness, explainability, accountability, and transparency can affect users' privacy-disclosure behavior; when algorithms lack these characteristics, algorithmic hegemony may emerge. On this basis, this study selects algorithm appreciation, algorithm aversion, and algorithmic

hegemony as the antecedent conditions of the algorithm dimension.

Algorithm appreciation refers to users' accepting attitude, recognition, or trust toward the recommendations and services provided by algorithms, manifested as relying on or tending to rely on algorithms in decision-making[20]. Some studies have pointed out that, once users become aware of the convenience and value brought by algorithms, they develop trust in algorithms and actively choose, adopt, and even depend on them[21]. When using library intelligent services, the degree of algorithm appreciation is directly related to users'acceptance of the processing of private information. When the degree of algorithm appreciation is high, users are more inclined to believe that algorithms can provide them with accurate intelligent search, personalized literature recommendations, and other services; they are therefore more willing to share private information such as borrowing preferences and search records, and their privacy boundaries will also display relatively relaxed characteristics. When the degree of algorithm appreciation is low, users will doubt the reliability and security of algorithms, may manage private information more cautiously, and their privacy boundaries will be relatively tightened; their trust in and acceptance of library intelligent services will also decline accordingly.

Algorithm aversion refers to users' negative emotions, negative attitudes, and avoidance tendencies toward the recommendations and services provided by algorithms[22]. Research shows that algorithm aversion can significantly trigger psychological reactance in individuals, thereby generating negative attitudes or behaviors[23]. In library intelligent services, in order to realize functions such as personalized recommendation and intelligent collection matching, algorithms continuously collect and use users' borrowing records, search trajectories, and other personal private information. This can easily arouse users' privacy concerns, which in turn fosters algorithm aversion, causing users to develop avoidance tendencies toward library intelligent algorithms. This will not only reduce their willingness to use the services and their overall evaluations, but will also lead them to actively tighten their privacy boundaries and restrict algorithms' access to and use of private information.

Algorithmic hegemony refers to the phenomenon in which users' autonomous right to choose information is forced to yield to algorithms[24]. Algorithmic hegemony is giving rise to an increasingly concealed and ubiquitous "digital Leviathan," posing severe challenges to the protection of users' private information. By comprehensively and continuously collecting users' browsing trajectories, reading duration, and even personal registration information, algorithms conduct deep processing and associative matching of data in order to provide services. For example, they may associate search trajectories with borrowing records to infer reading preferences, combine reading duration with collection types to define interest tags, and construct a complete portrait of user behavior through cross-matching multidimensional data, thereby quietly intervening in how users define the recipients and scope of sharing their private information. As a result, users' key rights to control and expand their privacy boundaries are

gradually taken over by algorithms, and users become manipulated individuals who have lost the right to choose information. Algorithmic hegemony invisibly expands users' privacy boundaries. Once users perceive that their private information has been violated, they may adopt conservative strategies and actively narrow their own privacy boundaries in order to resist algorithms' improper intervention in and excessive encroachment upon the private sphere.

2.3 Platform Dimension

CPM theory emphasizes the binary interactive nature of privacy, involving both the discloser and the recipient of information[25]. As the recipient of information, the platform provides users with diversified privacy-setting options[13], such as setting the visible scope of content and restricting the platform' s collection of browsing history. These privacy policies give users a relatively high degree of flexibility, enabling them to adjust the openness and degree of their privacy boundaries at any time according to their own needs. They therefore play an important role in alleviating users' privacy concerns and enhancing their willingness to disclose private information. On this basis, this study takes privacy policy as the antecedent condition of the platform dimension.

Privacy policy is a collaborative mechanism for privacy boundaries; it is the statement and notice made by a platform concerning how it protects user information when collecting, using, and sharing users' personal information[26]. CPM theory points out that confusion in privacy-boundary management often stems from failures in collaborative mechanisms, and existing studies have also confirmed that privacy policy is an important antecedent that promotes the formation of privacy boundaries. In library intelligent services, privacy policies clearly inform users of the categories of information collected and the specific scope of data processing

···and methods, and protective measures for private information; it serves as an action guide for libraries to regulate the privacy management of intelligent services. A sound privacy policy for library intelligent services can eliminate users' privacy concerns through explicit boundary agreements, effectively enhance users' trust in the service, and thereby encourage users to actively broaden their privacy boundaries and voluntarily share relevant private information in order to obtain library intelligent services that better meet their own needs.

2.4 Conceptual Model

Based on the above discussion, this study takes library intelligent services as the specific context and divides the factors influencing users' privacy boundaries into three core dimensions: users, algorithms, and platforms. Among them, the user dimension includes three variables—privacy value tendency, perceived privacy risk, and perceived privacy control—which constitute the core basis for users' subjective cognition and decision-making and directly affect the construction logic of their privacy boundaries. The algorithm dimension includes three vari-

ables—algorithm appreciation, algorithm aversion, and algorithmic hegemony—which adjust privacy boundaries by influencing users' acceptance of and trust in library intelligent-service algorithms. The platform dimension takes privacy policy as its core variable; as an institutional norm for library intelligent services, it provides clear reference bases and behavioral rules for users' autonomous setting of privacy boundaries. Accordingly, the conceptual model of factors influencing users' privacy boundaries in library intelligent services constructed in this study is shown in Figure 1.

Figure contents: user dimension—perceived privacy risk (PR), perceived privacy control (PC), privacy value tendency (PVT); algorithm dimension—algorithm appreciation (AP), algorithm aversion (AV), algorithmic hegemony (AH); platform dimension—privacy policy (PP); configurational effect; privacy boundary (PD).

Figure 1 Conceptual model of factors influencing users'privacy boundaries in library intelligent services

3 Research Design for Factors Influencing Users' Privacy Boundaries in Library Intelligent Services

3.1 Research Method

Qualitative Comparative Analysis (QCA) is based on Boolean algebra and uses set-theoretic thinking to examine the mechanism by which combinations of antecedent conditions affect the explained variable in complex social phenomena[27]. Fuzzy-set Qualitative Comparative Analysis (fsQCA) is one of the main variants of QCA. It combines fuzzy sets and fuzzy logic with QCA, supports continuous assignment of research variables within the interval $[0, 1]$, is applicable to different sample sizes and data types, and can also identify all equivalent combinations of conditions that lead to an outcome. Users' privacy boundaries in library intelligent services constitute a complex and multidimensional issue that is susceptible to the interactive influence of multiple factors; meanwhile, because of the sensitivity of privacy issues, survey data often contain considerable ambiguity and uncertainty. Compared with traditional statistical methods, fsQCA provides a more appropriate methodological path for analyzing this issue.

3.2 Questionnaire Design

The questionnaire consists of two parts: the first part collects basic information about the respondents, and the second part is a measurement scale for factors influencing users' privacy boundaries in library intelligent services. The scale was developed on the basis of mature scales and revised according to the specific context of this study, with the aim of ensuring good reliability and validity. The questionnaire adopts a five-point Likert scale, where "1" indicates "strongly disagree" and "5" indicates "strongly agree." To ensure the reliability of the

questionnaire, this study conducted a pilot survey before formally releasing the questionnaire, adjusted the questionnaire according to respondents' feedback, and finally formed the formal scale shown in Table 1.

Table 1 Measurement Scale and Reference Sources

Variable	Item	Measurement item	Reference source
Privacy value tendency (PVT)	PVT1	Compared with others, when using library intelligent services, I pay more attention to protecting personal private information.	Xu H et al.[16]
Privacy value tendency (PVT)	PVT2	Compared with others, when using library intelligent services, I am more worried that my personal private information will be threatened.	Xu H et al.[16]
Privacy value tendency (PVT)	PVT3	Compared with others, when using library intelligent services, I am more concerned about how the library uses personal private information.	Xu H et al.[16]

Variable	Item	Measurement item	Reference source
Privacy value tendency (PVT)	PVT4	Compared with others, when using library intelligent services, I am more sensitive to the platform' s requirement that I provide private information.	Xu H et al.[16]
Perceived privacy risk (PR)	PR1	I feel that the risk of privacy leakage is very high when using library intelligent services.	Yang Xuanhui et al.[28]; Lu Nan et al.[29]; Li Yingying et al.[30]
Perceived privacy risk (PR)	PR2	I feel that providing personal private information when using library intelligent services may produce negative consequences.	Yang Xuanhui et al.[28]; Lu Nan et al.[29]; Li Yingying et al.[30]
Perceived privacy risk (PR)	PR3	I feel that, when using library intelligent services, the platform uses my private information without fully informing me or without my explicit authorization.	Yang Xuanhui et al.[28]; Lu Nan et al.[29]; Li Yingying et al.[30]

Variable	Item	Measurement item	Reference source
Perceived privacy risk (PR)	PR4	I feel that I will be tracked and monitored when using library intelligent services.	Yang Xuanhui et al.[28]; Lu Nan et al.[29]; Li Yingying et al.[30]
Perceived privacy control (PC)	PC1	I believe that I can decide whether to provide private information to library intelligent services.	Zhu Hou et al.[31]; Sun Wei et al.[32]
Perceived privacy control (PC)	PC2	I believe that I can clearly understand which private information of mine is used by library intelligent services.	Zhu Hou et al.[31]; Sun Wei et al.[32]
Perceived privacy control (PC)	PC3	I believe that I can clearly understand how library intelligent services use my private information.	Zhu Hou et al.[31]; Sun Wei et al.[32]
Perceived privacy control (PC)	PC4	I believe that I can effectively protect the private information I disclose to library intelligent services.	Zhu Hou et al.[31]; Sun Wei et al.[32]

Variable	Item	Measurement item	Reference source
Algorithm appreciation (AP)	AP1	I think the content recommended to me by library intelligent services basically meets my needs.	Le Chengyi et al.[20]; Xie Jingzhong et al.[22]; Li Guihua et al.[33]
Algorithm appreciation (AP)	AP2	I think the content provided by library intelligent services is relatively novel and interesting.	Le Chengyi et al.[20]; Xie Jingzhong et al.[22]; Li Guihua et al.[33]
Algorithm appreciation (AP)	AP3	I think library intelligent services enable me to quickly filter and find content that interests me.	Le Chengyi et al.[20]; Xie Jingzhong et al.[22]; Li Guihua et al.[33]
Algorithm appreciation (AP)	AP4	I think library intelligent services are trustworthy.	Le Chengyi et al.[20]; Xie Jingzhong et al.[22]; Li Guihua et al.[33]

Table 1 (continued)

Variable	Item	Statement	Reference source
Algorithm aversion (AV)	AV1	I feel somewhat uncomfortable that library intelligent services can accurately grasp my reading preferences.	Le Chengyi et al. [20]; Zhang Ning et al. [34]
Algorithm aversion (AV)	AV2	I feel somewhat concerned that library intelligent services collect my private information.	Le Chengyi et al. [20]; Zhang Ning et al. [34]
Algorithm aversion (AV)	AV3	I have concerns about possible leakage of private information or security risks that may be brought about by library intelligent services.	Le Chengyi et al. [20]; Zhang Ning et al. [34]
Algorithm aversion (AV)	AV4	I worry that library intelligent services may use my private information for other purposes.	Le Chengyi et al. [20]; Zhang Ning et al. [34]

Variable	Item	Statement	Reference source
Algorithmic hegemony (AH)	AH1	When using library intelligent services, I need to accept and agree to certain agreements before I can obtain the relevant services.	Xie Jingzhong et al. [22]; Zha Daolin et al. [35]
Algorithmic hegemony (AH)	AH2	When using library intelligent services, I am required to fill in detailed personal information.	Xie Jingzhong et al. [22]; Zha Daolin et al. [35]
Algorithmic hegemony (AH)	AH3	When using library intelligent services, the information I receive is basically determined by the library intelligent services rather than based on my personal choices.	Xie Jingzhong et al. [22]; Zha Daolin et al. [35]

Variable	Item	Statement	Reference source
Algorithmic hegemony (AH)	AH4	When using library intelligent services, I cannot know the operating principles of the library intelligent services and can only accept them passively.	Xie Jingzhong et al. [22]; Zha Daolin et al. [35]
Privacy policy (PP)	PP1	The privacy policy of library intelligent services clearly stipulates the ways and purposes for which the private information I provide will be used.	Li K et al. [36]; Zhu Hou et al. [31]; Yang Ruixian et al. [37]
Privacy policy (PP)	PP2	The privacy policy of library intelligent services can help me clarify my rights with respect to privacy protection.	Li K et al. [36]; Zhu Hou et al. [31]; Yang Ruixian et al. [37]

Variable	Item	Statement	Reference source
Privacy policy (PP)	PP3	When my private information is infringed upon, the privacy policy of library intelligent services can provide me with effective solutions.	Li K et al. [36]; Zhu Hou et al. [31]; Yang Ruixian et al. [37]
Privacy policy (PP)	PP4	The privacy policy of library intelligent services is an effective way to protect my private information.	Li K et al. [36]; Zhu Hou et al. [31]; Yang Ruixian et al. [37]
Privacy boundary (PD)	PD1	I agree that library intelligent services may record and analyze my private information for the daily management of the library.	Xie Zhen et al. [38]; Tong Yunfeng et al. [39]
Privacy boundary (PD)	PD2	I agree that library intelligent services may record and analyze my private information to provide personalized services.	Xie Zhen et al. [38]; Tong Yunfeng et al. [39]

Variable	Item	Statement	Reference source
Privacy boundary (PD)	PD3	I agree that library intelligent services may collect and analyze my private information in a way that does not reveal my identity.	Xie Zhen et al. [38]; Tong Yunfeng et al. [39]
Privacy boundary (PD)	PD4	I agree that library intelligent services may process my private information within a necessary scope to ensure the safety and convenience of my use of the services.	Xie Zhen et al. [38]; Tong Yunfeng et al. [39]

3.3 Samples and Data Collection

This study obtained empirical data by distributing an online questionnaire. A convenience sampling method was adopted. With the assistance of the Wenjuanxing platform, the questionnaire was distributed through WeChat group chats, QQ group chats, Xiaohongshu, and reposts on WeChat Moments. The survey period was from November 26 to December 4, 2024. A total of 484 questionnaires were collected. After excluding 66 invalid questionnaires—including those from respondents who had not used library intelligent services, those with excessively short completion times, those in which the same option was selected throughout, or those with obvious logical contradictions—418 valid questionnaires were ultimately obtained, with an effective response rate of 86.36%. The demographic information of the respondents is shown in Table 2.

Table 2 Respondents' Demographic Information

Item	Option	Frequency	Percentage
Gender	Male	183	43.78%
Gender	Female	235	56.22%
Age	20 years old and below	114	27.27%
Age	21–25 years old	213	50.96%
Age	26–30 years old	71	16.98%
Age	31–35 years old	14	3.35%
Age	36 years old and above	6	1.44%
Education level	Junior college and below	50	11.96%
Education level	Undergraduate	236	56.46%
Education level	Master' s student	107	25.60%
Education level	Doctoral student	25	5.98%

Table 2 (continued)

Item	Option	Frequency	Percentage
Frequency of using library intelligent services	Less than once per week	98	23.44%
Frequency of using library intelligent services	1–3 times per week	176	42.11%
Frequency of using library intelligent services	4–5 times per week	77	18.42%
Frequency of using library intelligent services	6–7 times per week	67	16.03%

3.4 Reliability Test

Reliability is an important indicator for evaluating the stability and internal consistency of a scale. This study uses the Cronbach' s α coefficient to measure the reliability of the scale [40]. As shown in Table 3, the Cronbach's α coefficients of the variables range from 0.811 to 0.891, indicating that the scale has good reliability.

Table 3 Reliability Test

Variable	Cronbach' s α
PVT	0.819
PR	0.891
PC	0.817
AP	0.818
AV	0.873
AH	0.811
PP	0.873
PD	0.818

On the premise that reliability met the requirements, this study first used the KMO statistic and Bartlett's test of sphericity to determine whether factor analysis was appropriate. The results showed that the KMO value was 0.898, and the chi-square value of Bartlett' s test of sphericity was 7,147.786, with significance less than 0.001, indicating that the data were suitable for factor analysis. Principal component analysis was then adopted, common factors were extracted according to the criterion of eigenvalues greater than 1, and the orthogonal rotation method with maximum variance was used to obtain the factor loadings of each item. A total of 8 common factors were extracted, with a cumulative variance contribution rate of 69.446%, meeting the requirement of being greater than 50.0%; after rotation, the factor loadings of all items were greater than 0.5. Thus, the questionnaire items showed an ideal aggregation effect, the dimensions were clearly distinguished, and the scale had good structural validity.

This study further examined the convergent validity of the scale through standardized factor loadings, composite reliability (CR), and average variance extracted (AVE)[41]. As shown in Table 4, the standardized factor loadings of all variables were greater than 0.6, the CR values ranged from 0.811 to 0.893, and all AVE values were greater than 0.5, all reaching the criteria for convergent validity. As shown in Table 5, the square roots of the AVE values were all greater than the correlation coefficients among variables, indicating that the scale had good discriminant validity[42].

Table 4 Convergent Validity Test

Variable	Item	Standardized Factor Loading	CR	AVE
PVT	PVT1	0.754	0.821	0.534
PVT	PVT2	0.713	0.821	0.534
PVT	PVT3	0.747	0.821	0.534
PVT	PVT4	0.709	0.821	0.534
PR	PR1	0.872	0.893	0.675
PR	PR2	0.797	0.893	0.675
PR	PR3	0.822	0.893	0.675
PR	PR4	0.794	0.893	0.675

Variable	Item	Standardized Factor Loading	CR	AVE
PC	PC1	0.619	0.820	0.534
PC	PC2	0.781	0.820	0.534
PC	PC3	0.784	0.820	0.534
PC	PC4	0.726	0.820	0.534
AP	AP1	0.750	0.819	0.531
AP	AP2	0.701	0.819	0.531
AP	AP3	0.762	0.819	0.531
AP	AP4	0.700	0.819	0.531
AV	AV1	0.724	0.877	0.641
AV	AV2	0.836	0.877	0.641
AV	AV3	0.828	0.877	0.641
AV	AV4	0.809	0.877	0.641
AH	AH1	0.613	0.811	0.521
AH	AH2	0.650	0.811	0.521
AH	AH3	0.817	0.811	0.521
AH	AH4	0.786	0.811	0.521

Table 4 (continued)

Variable	Item	Standardized Factor Loading	CR	AVE
PP	PP1	0.821	0.874	0.635
PP	PP2	0.754	0.874	0.635
PP	PP3	0.825	0.874	0.635
PP	PP4	0.785	0.874	0.635
PD	PD1	0.734	0.818	0.530
PD	PD2	0.711	0.818	0.530
PD	PD3	0.740	0.818	0.530
PD	PD4	0.726	0.818	0.530

Table 5 Correlation Coefficient Matrix and AVE Square-Root Test

	PVT	PR	PC	AP	AV	AH	PP	PD
PVT	0.731							
PR	0.382	0.822						
PC	0.458	0.153	0.731					
AP	0.524	0.159	0.593	0.729				
AV	0.464	0.686	0.135	0.205	0.800			
AH	0.385	0.571	0.241	0.372	0.513	0.722		
PP	0.407	0.166	0.525	0.706	0.219	0.244	0.797	
PD	0.423	0.157	0.591	0.605	0.156	0.393	0.466	0.728

3.5 Common Method Bias Test

This study used Harman's single-factor method to test for common method bias, conducting unrotated principal component factor analysis on all measurement items. The results showed that there were 8 factors with eigenvalues greater than 1, and the variance explained by the first factor was 28.395%, lower than the test threshold standard of 40%[43], indicating that there was no serious common method bias in this study.

4 Analysis of Factors Influencing the Privacy Boundaries of Users of Library Intelligent Services Based on fsQCA

4.1 Variable Calibration

Because the dataset for fsQCA analysis must be a fuzzy set defined within the interval $[0, 1]$, the data need to be calibrated before the specific analysis[44]. This study adopted the direct calibration method: first, the mean value of each item was calculated to construct the initial dataset for each variable; then, using a logistic function, the initial data were calibrated according to three qualitative anchors—full membership, crossover point, and full non-membership. During the calibration process, 95%, 50%, and 5% were used as the anchors for full membership, crossover point, and full non-membership, respectively[45], thereby completing the calibration of all variables.

4.2 Necessity Analysis

To identify whether a single antecedent variable constitutes a necessary condition for the privacy boundary of users of library intelligent services, necessity analysis is required. Generally, if the consistency threshold of an antecedent variable exceeds 0.9, it can be determined to be a necessary condition for the outcome variable[46]. According to Table 6, the consistency thresholds of all antecedent variables did not exceed 0.9, indicating that there was no

necessary conditions affecting users' privacy boundaries in library intelligent services. This result confirms the complex nature of the synergistic effects of multiple conditions: the opening of users' privacy boundaries depends on the configurational linkage among users themselves, algorithms, and platforms.

4.3 Robustness Test

To further verify the stability and validity of the research findings, this study conducted a robustness test by adjusting the consistency threshold[47]. After raising the consistency threshold from 0.8 to 0.85, the configurational analysis was performed again. The results show that the combinations of core conditions in the configurational paths are consistent with the original findings, and that both the overall consistency and the overall coverage remain unchanged. Therefore, the findings of this study exhibit strong robustness.

Table 6 Necessary Condition Analysis

Antecedent condition	Consistency	Coverage
PVT	0.800	0.759
~PVT	0.561	0.706
PR	0.682	0.727
~PR	0.632	0.694
PC	0.756	0.815
~PC	0.615	0.667
AP	0.766	0.792
~AP	0.575	0.652
AV	0.693	0.715
~AV	0.621	0.705
AH	0.718	0.771
~AH	0.624	0.680
PP	0.763	0.810
~PP	0.609	0.671

Note: "~" denotes logical "not."

4.4 Configurational Analysis

Through fsQCA analysis, three types of solutions can be obtained: the intermediate solution, the complex solution, and the parsimonious solution. The intermediate solution both conforms to theoretical expectations and is supported by empirical evidence, while also having moderate complexity; it is therefore regarded as the preferred option for interpreting results. In selecting case frequency, the minimum threshold must be set according to the total sample size and the distribution of cases across configurations—usually taking 1 as the minimum threshold—and the selected frequency should generally cover at least 75% of the observed cases. The consistency threshold determines the explanatory strength of antecedent-condition configurations for the outcome; 0.75 is regarded as the minimum consistency threshold[48]. The sample size in this study is a large sample. Based on the data distribution, the case-frequency threshold was set to 5, the consistency threshold to 0.8, and the PRI consistency threshold to 0.7.

Based on the above criteria, this study identified two types of configurational paths for users' privacy boundaries in library intelligent services: open-type privacy boundaries and closed-type privacy boundaries. Ultimately, 8 condition configurations affecting the outcome variable were formed, as shown in Table 7. Among them, 7 configurational paths were obtained for open-type privacy boundaries. The consistency of both the individual solutions and the overall solution is higher than 0.8, the overall coverage is 0.604, and the raw coverage

of each configuration is around 30%, indicating relatively balanced explanatory power. Moreover, all take perceived privacy control as the core condition, making it the key factor driving users to open their privacy boundaries. For closed-type privacy boundaries, only 1 configurational path exists. Its raw coverage, unique coverage, and overall coverage are all 0.402, indicating that it is a sufficient condition leading users not to open their privacy boundaries; it can independently explain 40.2% of the variation in closed-type cases, with no other equivalent configurations.

Table 7 Configurational Paths of Factors Influencing Users' Privacy Boundaries in Library Intelligent Services

Antecedent condition	Open-type privacy boundary — Configuration 1	Open-type privacy boundary — Configuration 2	Open-type privacy boundary — Configuration 3	Open-type privacy boundary — Configuration 4	Open-type privacy boundary — Configuration 5	Open-type privacy boundary — Configuration 6	Open-type privacy boundary — Configuration 7	Closed-type privacy boundary — Configuration 8
PVT					•			
PR						•		
PC								
AP	•	•	•					
AV				•	•	•	•	
AH							•	
PP		•	•		•	•	•	
Raw coverage	0.302	0.325	0.317	0.395	0.396	0.394	0.382	0.402
Unique coverage	0.011	0.034	0.028	0.022	0.013	0.024	0.010	0.402
Consistency	0.962	0.962	0.973	0.959	0.951	0.940	0.944	0.956
Overall coverage	0.604	0.604	0.604	0.604	0.604	0.604	0.604	0.402
Overall consistency	0.926	0.926	0.926	0.926	0.926	0.926	0.926	0.956

Note: and • respectively indicate the presence of a core condition and an auxiliary condition; and respectively indicate the absence of a core condition and an auxiliary condition; a blank cell indicates that the antecedent condition may be present or absent.

5 Discussion and Analysis

This study classifies the eight configurational paths above into five types according to shared core conditions: algorithm-trust acceptance, hegemony–value balancing, risk-perception balancing, complex privacy cognition, and value–algorithm indifference.

5.1 Algorithm-Trust Acceptance Type

This type of configurational path includes Configuration 1 (`PVT * \sim PR * PC * AP * \sim AV * \sim AH`) and Configuration 2 (`\sim PR * PC * AP * \sim AV * \sim AH * PP`), with high perceived privacy control and low algorithm aversion as the core conditions. Users of this type exhibit high perceived privacy control and high algorithm appreciation, low perceived privacy risk, low algorithm aversion, and low algorithmic hegemony, while also showing either a relatively strong privacy-value orientation or recognition of privacy policies; consequently, they tend to open their privacy boundaries. This willingness may be related to users' experience with intelligent services. As usage experience accumulates, users may more accurately evaluate their own capabilities and the effectiveness of algorithms, believe that they can effectively control the flow and use contexts of their private information, and gradually experience less aversion to algorithms, thereby becoming more willing to accept intelligent services. Therefore, in appropriate contexts, to fully enjoy the convenience of library intelligent services, such users are more inclined to actively disclose personal private information.

In view of this, library intelligent services should rely on intelligent technologies to collect real-time data on users' in-library behavior, search records, borrowing preferences, and the like, and use algorithmic models to accurately anticipate user needs, thereby realizing the algorithmic proactive capture of service needs and intelligent responses. For example, intelligent navigation robots can match users' locations with their search needs through algorithms and proactively guide them along collection-search paths; personalized recommendation algorithms can automatically push suitable resources such as books, journals, and electronic documents when users enter the search interface or arrive at a collection area in the library; and intelligent question-answering algorithms can proactively capture users' consultation needs through voice, text, and other interactive modes, answering questions in real time about literature searches, space reservations, and related matters, so as to build a personalized service system that meets users' needs and enhances user experience and well-being.

5.2 Hegemony-Value Balancing Type

This type of configurational path includes Configuration 3 (PVT * \sim PR * PC * AP * AH * PP) and Configuration 6 (PVT * PR * PC * AV * AH * PP), with high privacy-value orientation, high perceived privacy control, and high algorithmic hegemony as the core conditions. When users have a high privacy-value orientation, high perceived privacy control, high algorithmic hegemony, and high recognition of privacy policies, and are accompanied by relatively high algorithm appreciation or algorithm aversion, they are more inclined to disclose personal privacy. Although such users attach great importance to their own privacy, their strong perceived ability to control privacy enhances their trust in intelligent services and thus weakens their original privacy-value orientation. Although they clearly recognize the prevalence of algorithmic hegemony, because of considerations such as service-use needs, the high cost of resistance, or the limited effectiveness of resistance, after weighing the pros and cons these users choose to adopt algorithm-adaptive behaviors[22] and accept and use algorithm-recommended services.

Therefore, library intelligent services should clearly disclose, in a standardized form, the principles, application purposes, and operating mechanisms of algorithms, helping users understand the logic of algorithmic decision-making and alleviating their perception of algorithmic hegemony. At the same time, technological means should be used to strengthen users' ability to control privacy, including functions such as tiered privacy authorization and traceability of data use, guiding users to domesticate technology through the rights conferred by technology and to reshape their subject position by adjusting algorithmic recommendation preferences and restricting the information obtained by platforms. In addition, the boundaries of privacy-data collection and use must be strictly defined, algorithmic-hegemony behaviors should be avoided, and a transparent and secure intelligent service environment should be constructed, so as to balance users' demands for privacy protection with their need to use algorithmic services.

5.3 Risk-Perception Balancing Type

This type of configurational path includes Configuration 5 (PVT * PR * PC * AP * AV * PP) and Configuration 7 (PR * PC * AP * AV * AH * PP), with high perceived privacy risk, high perceived privacy control, and high algorithm appreciation as the core conditions. When users have high perceived privacy risk, high perceived privacy control, high algorithm appreciation, and high recognition of privacy policies, and are accompanied by a relatively strong privacy-value orientation or algorithmic hegemony, they will choose to open their privacy boundaries. Existing studies have pointed out that stronger perceived privacy control makes users more confident that they can effectively control the use and dissemination of private information[15]. Although dealing with privacy issues requires more energy and time, in contexts of high perceived privacy risk users are more inclined to rely on their own capabilities to cope with them, which to a

certain extent confirms the privacy-paradox phenomenon[15]. The service convenience, efficiency improvements, and satisfaction of personalized needs brought about by algorithms significantly enhance users' recognition and appreciation; a relatively high level of algorithm appreciation prevents their behavior of using library intelligent services from being affected by algorithm aversion.

For such users, library intelligent services can be optimized in three respects. First, privacy data should be collected in accordance with the principle of minimum necessity, and users' identity information should be anonymized through de-identification, encryption, and related processing, so as to reduce privacy risks caused by improper information use or sharing. Second, users' right to know should be guaranteed by regularly disclosing data-security measures and algorithm-operating logic through various channels, thereby consolidating, through transparent management across the entire process, the foundation of users' trust in library algorithmic services. Third, privacy-literacy education should be carried out: users' levels of privacy literacy can be assessed through questionnaires, and the importance of privacy protection and practical techniques can be popularized among users.

5.4 Complex Privacy Cognition Type

This type of configurational path includes only Configuration 4 (`PVT * PR * PC * AP * AV * AH`), jointly composed of high privacy-value orientation, high perceived privacy risk, high perceived privacy control, high algorithm appreciation, high algorithm aversion, and high algorithmic-hegemony behavior. Except for algorithm aversion and privacy policy, all other conditions are core conditions. Users of this type attach great importance to privacy value and have a clear understanding of algorithmic hegemony. However, the outstanding performance of algorithms in personalization and efficient services significantly improves user experience, causing them to develop trust in algorithms and to tend, on the premise of safeguarding privacy

pursue more efficient and more personalized services. Because privacy management requires considerable effort and time, even when users perceive privacy risks to be high, they may not readily take action. This may be related to optimistic bias: individuals often believe that their own risk of experiencing negative events is lower than that of others, and optimistic bias can also weaken the negative effect of algorithm aversion on service use[20]. With a high sensitivity to, and strong control over, the flow and use of private information, such users will moderately relax their privacy boundaries in order to enjoy the convenience brought by smart library services.

In response, libraries should simplify the design of system-permission functions and grant users greater operational autonomy—for example, by giving users the ability to view, modify, and delete personal information at any time and to refuse personalized customization—thereby effectively improving users' perceived level of privacy control. At the same time, libraries should establish an

end-to-end algorithm supervision mechanism, strictly control excessive algorithmic intervention in resource recommendations, avoid the "information cocoon" problem caused by homogenized recommendations, and weaken the negative effects brought by algorithms. In addition, through educational resources such as online courses and interactive tutorials, libraries can popularize methods for coping with privacy risks, dispel risk neglect caused by optimistic bias, and ultimately build a transparent, secure, efficient, and convenient smart-service environment.

5.5 Value–Algorithm Indifference Type

This configurational path includes Configuration 8 (`~PVT * ~PR * ~PC * AP * ~AV * ~AH * ~PP`), whose core conditions are low privacy-value orientation, low algorithm appreciation, and low algorithm aversion. Users of this type have no clear tendency to protect private information; toward smart-service algorithms, they show neither appreciation and reliance nor aversion and avoidance. They are characterized by vague perception of privacy value and a neutral attitude toward algorithms. This result is consistent with the logic in CPM theory that "identification with privacy value is the underlying motivation for boundary disclosure" [49], and it also accords with the attributes of libraries as public cultural service institutions: the reading, retrieval, and other data involved are weakly private information, and the public-welfare nature of libraries makes it difficult for such users to develop a high-value perception of privacy. Meanwhile, users'neutral attitude of neither appreciating nor disliking algorithms[50] further dissolves the external motivation for opening privacy boundaries, ultimately forming a dual logic of "no motivation and no need."

For this type of user, smart library services may follow the principles of low intervention, light personalization, and implicitness. On the service side, libraries can adopt an implicit data-use model and, based on users' objective usage behavior, carry out lightweight basic intelligent adaptation—for example, ranking search results by frequency of use and matching collection recommendations with the disciplinary fields to which users belong—so as to avoid arousing user resentment through frequent pop-up privacy-authorization prompts. Libraries can create de-algorithmized basic services by integrating intelligent functions into basic scenarios such as retrieval and borrowing reminders, thereby weakening the perceived presence of algorithms. They can also set up a minimalist default low-permission privacy mechanism, simplify the user authorization process, and lower the threshold for use. In addition, lightweight access points for privacy and algorithm literacy can be established, with low-frequency dissemination of relevant content such as data-use norms and privacy-protection tips, leaving users to learn independently rather than imposing proactive push interventions.

6 Conclusion

Based on CPM theory, this study used the fsQCA method to conduct a configurational analysis of the factors influencing users' privacy boundaries in smart library services, yielding dual contributions and implications at both theoretical and practical levels. At the theoretical level, this study applied CPM theory to the specific digital-intelligent context of smart library services, deepening the explanatory power of the theory for users' privacy-management behavior in particular situations. Second, by incorporating algorithmic factors into the analytical framework of CPM theory, this study broke through the traditional research scope of interpersonal interaction and extended it to interaction scenarios between humans and intelligent systems, verifying the adaptability and extensibility of the theory in the digital-intelligent era. At the practical level, through configurational analysis, this study clarified the complex configurational paths and mechanisms by which multidimensional variables influence users' privacy boundaries, providing empirical support for libraries to accurately grasp the behavioral logic of users' privacy management in smart services. At the same time, by incorporating algorithmic factors into the scope of privacy-protection research, this study provides concrete operational ideas for libraries to optimize smart-service design and formulate targeted user-privacy protection strategies, and also offers useful reference and guidance for user-privacy protection practices across the broader field of smart services.

This study also has certain limitations. First, the factors considered in relation to users' privacy boundaries in smart library services are limited. Future research will continue to attend to additional influencing factors, such as privacy fatigue generated by frequent user–algorithm interaction, so as to explore the determinants of privacy boundaries more comprehensively. Second, this study did not consider the dynamic nature of privacy boundaries, such as boundary coordination and boundary turbulence. Future research will continue to explore dynamic changes in privacy boundaries and corresponding coping strategies.

References

[1] Clarivate. Pulse of the Library 2024 [EB/OL]. [2025-12-17]. https://clarivate.com/academia-government/wp-content/uploads/sites/3/dlm_uploads/Pulse-of-the-Library-Report-2024.pdf.

[2] Ma Xiangping. The present and future of smart library services [J]. New Century Library, 2023(12): 9–13.

[3] IFLA. IFLA Trend Report 2024: Facing the Future of Information with Confidence [EB/OL]. [2025-12-17]. https://repository.ifla.org/items/ae4dfcc0-8def-4318-8c4c-7f0507d15609.

[4] Qian Jinjin. A comparative study of research in the field of "artificial intelligence + libraries" at home and abroad—A map-based quantitative analysis using COOC and SPSS [J]. New Century Library, 2024(9): 88–97.

[5] Balyan R, Mccarthy K S, Mcnamara D S. Applying natural language processing and hierarchical machine learning approaches to text difficulty classification [J]. International Journal of Artificial Intelligence in Education, 2020(3): 337–370.

[6] Yang Qizhong. Copyright dilemmas and solutions for high-quality data mining in public libraries [J]. Library, 2025(10): 9–17.

[7] Wei Mingyuan, Luo Kunming, Tang Ming, et al. Application research on embedding large language models (LLMs) into scenario-based services of smart libraries [J]. Library Theory and Practice, 2025(1): 83–94.

[8] Sun Yusheng, Chen Sihao, Liu Tao, et al. Knowledge-graph-enabled smart library information [[unclear: reference title continues beyond the visible page]]

Recommendation framework and mechanism research [J]. *Research on Library Science*, 2025(10): 74–82.

[9] Wang Wenjin, Li Yunhao, Zhang Yin. Empirical study on instruction design and fine-tuning methods for document-image intelligent question answering with large language models [J]. *Digital Library Forum*, 2025(1): 11–21, 32.

[10] Wu Ningbo, Li Di, Yang Fan, et al. User privacy risks and governance strategies in provincial public libraries in China [J]. *Library Work and Study*, 2024(9): 36–45.

[11] Gu Wenhao, Fan Zhenjia, Fan Xinxin, et al. Research on personal data collection, compliant use, and management implications: Based on textual analysis of privacy policies of digital-resource providers [J]. *Information Studies: Theory & Application*, 2025(7): 56–64.

[12] Zhang Xiaowei. Risks and regulatory paths for protecting library readers' information in the context of generative AI [J]. *Library Work and Study*, 2025(6): 26–35.

[13] Petronio S. *Boundaries of Privacy: Dialectics of Disclosure* [M]. New York: State University of New York Press, 2002: 2–3.

[14] Sharma S, Crossler R E. Disclosing too much? Situational factors affecting information disclosure in social commerce environment [J]. *Electronic Commerce Research and Applications*, 2014(5): 305–319.

[15] Geng Ruili, Wang Yifan. Selection and influence of privacy management strategies among social media users: A quasi-experimental study [J]. *Library and Information Service*, 2024(3): 94–104.

[16] Xu H, Luo X, Carroll J M, et al. The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing [J]. *Decision Support Systems*, 2011(1): 42–52.

[17] Petronio S. *Balancing the Secrets of Private Disclosures* [M]. London: Lawrence Erlbaum Associates Press, 2000: 37–46.

[18] Yu L, Li H, He W, et al. A meta-analysis to explore privacy cognition and information disclosure of internet users [J]. *International Journal of Information Management*, 2020: 102015.

[19] Chang Y, Wong S F, Libaque-Saenz C F, et al. The role of privacy policy on consumers perceived privacy [J]. *Government Information Quarterly*, 2018(3): 445–459.

[20] Le Chengyi, Wang Zixin, Kong Weiwei. Algorithm appreciation VS algorithm aversion: Users' "algorithm paradox" under intelligent short-video recommendation [J]. *Journal of Intelligence*, 2024(8): 170–181.

[21] Chen Yunyi, Liang Shaobo. Research on the influencing factors of the "netborn generation' s" algorithm attitudes [J]. *Library Development*, 2025(6): 172–185.

[22] Xie Jingzhong, Zhang Mingyang. Acceptance, avoidance, and adaptation: A study on social media users'algorithm coping [J]. *Information Studies: Theory & Application*, 2024(11): 81–90.

[23] Zhang Wen, Xiao Zengrui, Lü Mingjie. Algorithm aversion: Theoretical framework and research prospects [J]. *Science and Society*, 2024(2): 77–97.

[24] Gui Xiaowei. Protection of digital human rights in a smart society: Theoretical construction based on the "capability approach" [J]. *Law Review*, 2023(1): 153–163.

[25] Jia S J, Chi O H, Lu L. Social robot privacy concern (srpc): Rethinking privacy concerns within the hospitality domain [J]. *International Journal of Hospitality Management*, 2024: 103853.

[26] Wang Qiuzhen, Ma Da, Yang Mengru, et al. Neuroprivacy: A new perspective on user information privacy behavior research [J]. *Journal of Zhejiang University (Humanities and Social Sciences)*, 2022(9): 114–132.

[27] Du Yunzhou, Jia Liangding. Configuration perspective and qualitative comparative analysis (QCA): A new path for management research [J]. *Management World*, 2017(6): 155–167.

[28] Yang Xuanhui, Yan Zhangkuan. Research on influencing factors of users' algorithm-avoidance behavior in online health communities under the CAC paradigm [J]. *Journal of Modern Information*, 2024(2): 130–141.

[29] Zhan Nan, Yan Xiangyu. Research on the influencing mechanism of e-commerce intelligent-recommendation users' willingness to disclose information privacy [J]. *Journal of Modern Information*, 2023(10): 35–53.

[30] Li Yingying, Chen Tingting, Sun Yuqi. Research on influencing factors of users' perceived privacy risk in intelligent recommendation on social media [J]. *Journal of Intelligence*, 2023(2): 151–157.

[31] Zhu Hou, Zhang Mingxin. Research on influencing factors and configuration effects of privacy-information setting behavior among mobile APP users [J]. *Information Science*, 2021(7): 54-62.

[32] Sun Wei, Zhao Hong, Zang Guoquan, et al. Research on social commerce users' willingness to disclose privacy from the dual-calculus perspective [J]. *Library and Information Service*, 2022(24): 64-75.

[33] Li Guihua, Wang Manjing. Rationality of personalized recommendation on content platforms: Constructs and effects [J]. *Journal of Modern Information*, 2025(3): 10-24.

[34] Zhang Ning, Chen Jiangling, Yuan Qinjian. The dilemma of integration and separation: Research on academic users' willingness to use AIGC technology under algorithmic alienation [J]. *Journal of Modern Information*, 2025(5): 34-48.

[35] Zha Daolin, Jiang Zhihui, Cao Gaohui. Research on the connotation and structural dimensions of information-system users' perceived algorithm anxiety [J]. *Information Science*, 2022(6): 66-73.

[36] Li K, Wang X, Li K, et al. Information privacy disclosure on social network sites: An empirical investigation from social exchange perspective [J]. *Nankai Business Review International*, 2016(3): 282-300.

[37] Yang Ruixian, Shen Jianing, Xu Fan, et al. Construction and empirical study of an evaluation-index system for privacy policies of social media APPs [J]. *Information Studies: Theory & Application*, 2023(1): 81-89.

[38] Xie Zhen, Yang Jiulong. Users' willingness to disclose privacy from the perspective of smart libraries [J]. *Library Tribune*, 2020(9): 69-78.

[39] Dong Yunfeng, Zhang Xuebin. Equal protection of library readers' borrowing information and sensitive personal information [J]. *Library Work and Study*, 2023(12): 22-30.

[40] Devellis R F. *Scale Development: Theory and Applications* [M]. London: Sage, 1991: 26-39.

[41] Wu Minglong. *Structural Equation Modeling: Operation and Application of AMOS* [M]. Chongqing: Chongqing University Press, 2010: 212-216.

[42] Ye Fengyun, Chang Lin, Ye Yuxin, et al. Research on social-network users' false-information disclosure behavior: From the dual-path perspective of cognition and emotion [J]. *Library and Information Service*, 2024(21): 79-92.

[43] Podsakoff P M, Mackenzie S B, Lee J Y, et al. Common method biases in behavioral research: A critical review of the literature and recommended remedies [J]. *Journal of Applied Psychology*, 2003(5): 879-903.

[44] Chi Maomao, Du Yunzhou, Wang Weijun. Configuration perspective and qualitative comparative analysis method: A new path for empirical research in

library and information science [J]. *Journal of the China Society for Scientific and Technical Information*, 2021(4): 424–434.

[45] Schneider C Q, Rohlfing I. Case studies nested in fuzzy-set QCA on sufficiency: Formalizing case selection and causal inference [J]. *Sociological Methods & Research*, 2016(3): 526–568.

[46] Park Y K, El Sawy O A, Fiss P C. The role of business intelligence and communication technologies in organizational agility: A configurational approach [J]. *Journal of the Association for Information Systems*, 2017(9): 648–686.

[47] Zhang Ming, Du Yunzhou. Application of the QCA method in organization and management research: Positioning, strategies, and directions [J]. *Chinese Journal of Management*, 2019(9): 1312–1323.

[48] Campbell J T, Sirmon D G, Schijven M. Fuzzy logic and the market: A configurational approach to investor perceptions of acquisition-announcements [J]. *Academy of Management Journal*, 2016(1): 163–187.

[49] Liu Bailing, Sun Wenjing. A process study of mobile users' information-disclosure decisions from the holistic perspective of communication privacy management theory [J]. *Management Science*, 2021(6): 76–87.

[50] Wang Yajuan. Technological regulation, bodily return, and intelligent awakening: Three research orientations in the ethics of intelligent advertising [J]. *Modern Communication (Journal of Communication University of China)*, 2021(9): 130–134.

(Continued on p. 69)

[J]. *Library Research and Work*, 2025(6): 54–60, 68.

[27] Luo Qiangqiang, Zheng Lijuan, Guo Wenshan, et al. "Digital survival" of the "silver-haired group": the mechanism by which digital literacy affects older adults' sense of digital gain [J]. *Library Tribune*, 2023(5): 130–139.

[28] Dai Yanqing, Zhang Mengge, Fu Rui, et al. A study on factors influencing older adults'participation in public digital cultural services: from the perspective of cognition and attitude [J]. *Library Work in Colleges and Universities*, 2024(2): 21–30.

[29] Zhang Jingjing, Zhang Wang. The internal mechanism and micro-level evidence of social interaction empowering older adults' digital integration [J]. *Journal of Yunnan Minzu University (Philosophy and Social Sciences Edition)*, 2025(3): 50–61.

[30] Yang Baoqiang, Zhong Manli. Empowerment and capacity enhancement: a long-term mechanism for rural older adults' integration into the digital society [J]. *Hunan Social Sciences*, 2024(1): 128–136.

[31] Liu Yanfeng. Calling for information care for the silver-haired: what public libraries should do, find difficult to do, and can do in age-friendly services [J].

New Century Library, 2025(2): 37–44.

[32] Cyberspace Administration of China. Action outline for improving digital literacy and skills for all [EB/OL]. [2026-03-11]. https://www.cac.gov.cn/2021-11/05/c_1637708867754305.htm.

[33] Shi Qinggong, Zhou Jie, Feng Wei. Bridging the silver digital divide: dilemmas, frameworks, and implementation paths for improving digital literacy among older groups [J]. *Library Work in Colleges and Universities*, 2025(1): 53–60.

[34] Yang Qiaoyun, Li Jiaying. How can digital inclusion for older adults be realized? A combined analysis based on grounded theory and fuzzy-set QCA of 37 cases in China [J/OL]. *Modern Information*, 1–13 [2026-04-15]. https://link.cnki.net/urlid/22.1182.G3.20260316.2031.002.

[35] Wei Yan, Yang Lihong, Guo Xinyu. Pension capital, endogenous motivation, and the digital divide among older adults [J]. *Northwest Population Journal*, 2024(1): 59–73.

[36] Liao Minxiu, Fu Wenjing. Investigation and analysis of digital literacy services for older adults in public libraries [J]. *Research on Library Science*, 2025(4): 85–102.

[37] Zhao Fayuan. Driving factors, problem review, and practical paths for the governance of information poverty among older adults in public libraries [J]. *Hebei Library Journal of Science and Technology*, 2026(1): 9–17, 51.

Capability and Endogenous Motivation: A Grounded Theory Study on Influencing Factors of Digital Integration of Migrant Elderly

Zhao Fayuan

Yunnan Provincial Library, Kunming, 650031

Abstract Migrant elderly are a special vulnerable group of mobile elderly formed by China' s urban-rural dual structure, and their digital integration is critical to individual quality of life and urban inclusive governance. This study selected 15 migrant elderly as research subjects, collected data through semi-structured interviews, and conducted coding analysis on the interview corpus using grounded theory. The results show that capability and endogenous motivation are the two core factors affecting the digital integration of migrant elderly. To address the predicament of their digital integration, efforts should be made to improve capability through material and economic support, community network assistance, digital literacy enhancement, and health condition improvement, and to activate endogenous motivation by eliminating age bias, reshaping social roles, and reducing family substitution.

Keywords Migrant elderly; Digital integration; Capability; Endogenous motivation; Grounded theory

(Continued from page 61)

Algorithmic Profiling and Privacy Safeguarding: Research on Influencing Factors and Path of User Privacy Boundaries in Library Intelligent Services

Jia Ruonan Su Qiya

School of Public Administration of Xiangtan University, Xiangtan, 411105

Abstract Exploring the factors influencing user privacy boundaries in library intelligent services in the era of digital intelligence helps safeguard users' privacy rights and improve the quality of intelligent services. This study constructs a conceptual model based on Communication Privacy Management (CPM) theory and adopts the fuzzy-set Qualitative Comparative Analysis (fsQCA) method to analyze the factors influencing user privacy boundaries in library intelligent services. The study finds that user privacy boundaries are influenced by multiple factors, including privacy value orientation, perceived privacy risk, perceived privacy control, algorithm appreciation, algorithm aversion, algorithm bias, and privacy policy. Among these, perceived privacy control is a key variable influencing user privacy boundaries in library intelligent services. User privacy boundary management strategies exhibit diverse characteristics.

Keywords Library intelligent services; Communication Privacy Management theory; Privacy boundary

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