Factors Influencing Willingness to Disclose Personal Information for Community Governance: An Analysis of Context and Individual Attributes (Postprint)

Authors: Zhang Yudong, Wang Qi, Qian Jing, Liu Yi

Date: 2023-04-01T16:02:56+00:00

Abstract

[Purpose/Significance] Under the situation where the COVID-19 pandemic has become increasingly normalized, the collection and utilization of personal information in community governance have significantly intensified. Based on privacy protection, how to construct more harmonious application scenarios for personal information is an urgent issue to be addressed in the modernization of community governance based on big data. [Method/Process] Adopting a residents' perspective, scenario variables for community governance are established from three dimensions: interest orientation, security relevance, and disclosure level. Questionnaire surveys are employed to analyze the influence mechanism of scenarios on information disclosure willingness, and combined with individual attribute characteristics, the patterns of information disclosure willingness among different characteristic groups are revealed, thereby discussing optimization suggestions for the application of personal information in community governance. [Results/Conclusions] The study indicates that, influenced by organizational citizenship behavior factors, residents demonstrate higher willingness to disclose personal information in public-benefiting scenarios with high security relevance; while personal information is utilized for community governance, introducing personalized service feedback facilitates improvement of information disclosure willingness; when communities collect personal data, they should tailor approaches to local circumstances according to the distribution of residents' individual attributes and address residents' concerns to the greatest extent possible.

Full Text

Research on Influencing Factors of Personal Information Disclosure Intention for Community Governance: An Analysis of Scenarios and Individual Attributes

Zhang Yudong, Wang Qi, Qian Jing, Liu Yi

Institute of Public Safety Research, Tsinghua University, Beijing 100084

Abstract: [**Purpose/Significance**] In the context of COVID-19 becoming normalized, community governance has significantly intensified the collection and use of personal information. A critical challenge for modernizing community governance based on big data is how to construct more harmonious personal information application scenarios while protecting privacy. [**Method/Process**] From the residents' perspective, this study sets scenario variables for community governance from three aspects: interest tendency, security relevance, and disclosure degree. Through questionnaire surveys, it analyzes the influence mechanism of scenarios on disclosure intention, reveals the patterns of information disclosure intention across different demographic groups by incorporating individual attribute characteristics, and discusses optimization recommendations for personal information application in community governance. [**Result/Conclusion**] The research shows that, influenced by organizational citizenship behavior (OCB) factors, residents demonstrate higher willingness to disclose personal information in public-benefit and high-security-related scenarios. When collecting personal data, communities should adapt measures to local conditions based on the distribution of residents' individual attributes and respond to residents' concerns as much as possible.

Keywords: post-pandemic era; community governance; personal information disclosure intention; scenario; individual attributes; organizational citizenship behavior

---

As the first line of defense in COVID-19 prevention and control, communities have reached unprecedented levels of collecting and using residents' personal information across various control stages to precisely monitor and prevent epidemic risks. For instance, under Level 1 emergency response, community personnel screening required active disclosure of sensitive private information such as "travel history" and "co-residents." Research indicates that COVID-19 may exist long-term [1]. As the post-pandemic era arrives with normalized epidemic conditions, many personal information-dependent prevention and control strategies have gradually become institutionalized in daily community governance work [2-3].

High-quality social development further requires communities to possess capabilities for precise prevention, localized disposal, and scientific management of various emergency risks. In the big data era, modern community governance

empowered by information technology has rapidly increased its dependence on personal information, gradually highlighting conflicts between personal information application and privacy protection. As personal information carries increasingly high value density and privacy sensitivity [6], incidents involving illegal transfer, resale, and disclosure of personal information have intensified, drawing public attention to privacy infringement risks. Big data technology has, to some extent, broken through traditional privacy right models [7], and technical anonymization has not been fully achieved. Privacy protection relies on imperfect institutions, leading to unprecedented public demand and willingness for personal information privacy protection. Consequently, various big data-based public management practices generally face the trade-off between privacy security and information value transformation [8-10].

However, public acquiescence to frequent personal information collection for epidemic prevention and control under abnormal conditions does not imply acceptance under normalized social order. Some controversies and conflicts indicate that the expansion of public power scope and relative reduction of personal rights and privacy risks during emergencies cannot be sustained long-term in normalized community governance [4-5]. Therefore, how to guarantee personal information application under new circumstances has become an urgent problem for community governance.

Beyond community prevention and control needs for COVID-19, economic and social development requires communities to have precise prevention, nearby disposal, and scientific management capabilities for various emergency risks. In the big data era, modern community governance empowered by information technology has rapidly increased dependence on personal information, with conflicts between personal information application and privacy protection gradually becoming prominent. As personal information carries increasingly high value density and privacy sensitivity [6], incidents involving illegal transfer, resale, and disclosure of personal information have intensified, drawing public attention to privacy infringement risks. Big data technology has, to some extent, broken through traditional privacy right models [7], and technical anonymization has not been fully achieved. Privacy protection relies on imperfect institutions, leading to unprecedented public demand and willingness for personal information privacy protection. Consequently, various big data-based public management practices generally face the trade-off between privacy security and information value transformation [8-10].

Future community governance will face two challenges: first, how to achieve essentialization of personal information privacy security; second, how to construct a harmonious “disclosure-collection” relationship for personal information. The former depends on data technology development and legal system improvement, while the latter is a strategic optimization issue that determines whether community governance can obtain trustworthy and effective personal information support.

Personal information disclosure intention relates to several factors including

trust relationship, privacy sensitivity, perceived risk, and perceived benefit [11-15]. Since personal information inherently involves privacy content related to personality rights and its intelligence value involves property rights [16-17], residents' decisions to disclose personal information typically involve weighing personality rights against property rights. According to privacy calculus theory, personal information disclosure intention is based on "rational person" assumptions for optimization or utility maximization judgments [18-19]. Perceived value theory posits that when individuals can obtain feedback on personalized needs, their subjective willingness to disclose personal information strengthens, with expected need satisfaction prioritized over privacy security considerations [20-21]. Obviously, for individuals, potential privacy security risk costs and direct or indirect benefits from disclosing personal information jointly influence personal information disclosure intention [22-23].

Differences in external environment and individual characteristics also indirectly affect personal information disclosure intention. Relevant regulations and policies [24], social and cultural background differences [25], and national rule-of-law development levels [26] are also considered factors influencing individual privacy attitudes, implying that Chinese residents' willingness to disclose personal information may have unique patterns. Personality differences lead to different attitudes toward privacy and varying intentions regarding personal information disclosure. For instance, personal information disclosure intention shows clear patterns of variation by gender [27-28], personality [29], and personal experience [30].

Additionally, certain specific situations and momentary emotions may affect trust relationships and perceived risk, thereby altering personal information disclosure intention [31]. For example, during major public health emergencies like COVID-19, Chinese citizens' willingness to disclose personal information for community epidemic prevention needs does not follow traditional patterns but rather reflects voluntary action to improve public health emergency efficiency. This behavior of disclosing personal information without explicit or direct confirmed return expectations not only results from institutional constraints but also demonstrates characteristics of Organizational Citizenship Behavior (OCB) [32-33]. As a natural organization formed based on shared residential areas, using personal information for epidemic prevention work pursues "public-benefit" results recognized by most residents. Whether OCB factors influence personal information application in community governance remains to be explored.

In summary, this study temporarily treats privacy security as an objective condition and constant, takes the actual needs of personal information application in community governance as guidance, combines traditional research approaches and conclusions, and fully considers potential OCB factor influences. It treats scenarios and residents' individual attributes as environmental and ontological factors affecting personal information disclosure intention, sets scenario variables, conducts questionnaire surveys, studies the influence mechanism of community governance scenarios on residents' willingness to disclose personal

information, and reveals coupling influence patterns across different resident attributes, aiming to provide scientific theoretical support for better application of residents' personal information in community governance.

2 Theoretical Foundation and Research Methods

2.1 OCB-Based Factor Analysis

OCB refers to a series of autonomous, informal cooperative behaviors by individuals in organizations related to tasks. These behaviors are often not constrained by organizational incentive systems or institutional regulations but can effectively improve overall organizational effectiveness. OCB is commonly used as an important theory in human resource management. However, beyond employee-organization relationships, residents' OCB in participating in community governance cannot be ignored. On one hand, in the "VUCA era" risk environment [34], community governance organizations' flexibility, innovation in governance models, and particularly rapid adaptability to emergent needs are crucial. On the other hand, with rapid technological development, community governance technologies continuously update, but the organizational system needs relatively stable forms to maintain basic credibility. Balancing the development "speed difference" between technology and institutions is critical. During this epidemic prevention and control process, many technologies that efficiently empowered community prevention through personal information relied on residents' cooperation in collecting and using personal information. Undoubtedly, without clear rights-responsibility norms or standard references for personal information disclosure, this non-self-interested and beyond-duty resident behavior overall improved community governance effectiveness. Similar issues abound in community governance processes, such as personal information application in community governance represented by "facial recognition" technology. Therefore, theoretically exploring residents' OCB in community governance can provide driving force for constructing harmonious "disclosure-collection" relationships for personal information and essentially improve community precision governance capabilities.

Factors influencing OCB include scenario and individual attribute variables. Individual attributes are passive objective conditions relative to community governance processes, while scenarios are key to intervening in OCB. Therefore, based on OCB characteristics including altruism, sportsmanship, organizational loyalty, organizational compliance, civic virtue, personal initiative, and self-development, and integrating actual needs for collecting residents' personal information for community governance, this study establishes three indicators—interest tendency, security relevance, and disclosure degree—to verify and analyze OCB factor influences contained in personal information application scenarios in community governance. The specific conceptual model is shown in Figure 1 [Figure 1: see original paper].

2.2 Variable Setting

This study selects "facial information," a widely used personal biometric information, to instantiate personal information categories and sets scenario variables from three aspects: interest tendency, security relevance, and disclosure degree.

x1: Interest Tendency Variable. Personal information disclosure intention often involves benefit outcomes, showing significant differences between self-interest and altruism scenarios. Therefore, this variable is set from the first angle of interest tendency. Community governance includes both public interest scenarios recognized by the majority and scenarios with self-interest and altruism nature. Thus, this study divides personal information disclosure scenarios for community governance from residents' standpoint into "self-interest," "altruism," and "public-benefit" as three values for this variable:

- **Self-interest Scenario:** In the set scenario, residents disclose personal information under self-interest motivation to directly obtain results that only benefit themselves. For example, using "facial payment" at vending machines essentially involves residents providing personal information to technology service companies in exchange for personal consumption service convenience.
- **Altruism Scenario:** In the set scenario, residents disclose personal information under altruistic motivation to only provide benefits to the other party without directly or indirectly obtaining self-beneficial results. For example, disclosing personal information to property management companies only unilaterally meets property company operational needs, with no direct benefit to individual residents.
- **Public-benefit Scenario:** In the set scenario, residents disclose personal information to directly obtain results beneficial to the public regardless of motivation. For example, for public safety protection needs, video surveillance systems installed in communities neither create benefits for specific objects nor directly feedback benefits to residents whose personal information is collected, thus having no obvious self-interest or altruism characteristics but effectively improving public area order for indirect benefit to all community residents.

x2: Security Relevance. During the COVID-19 pandemic, most Chinese residents could understand and cooperate with personal information collection requirements in community governance from a public safety perspective due to concerns about virus transmission risks. Although the current "disclosure-collection" relationship around epidemic prevention and control needs is overall stable, this model is not sustainable. Therefore, this study sets this variable from the second angle of security relevance to discuss the influence of security relevance of personal information application scenarios on disclosure intention.

x3: Disclosure Degree. The higher the degree of personal information disclosure, the greater the risk of privacy infringement. Therefore, the degree of

personal information disclosure affects residents' willingness to disclose, making it the third angle variable set in this study.

2.3 Questionnaire Design

This study adopts a non-scale questionnaire survey to observe variable influence relationships regarding personal information disclosure intention. Based on field surveys in a Beijing community, questions representing interest tendency, security relevance, and personal information disclosure degree were designed and revised through expert consultation and pre-testing/blind testing to produce the final questionnaire. The frequency of options corresponding to different disclosure attitudes is used to characterize the group tendency quantification results of community residents' personal information disclosure intention. Higher frequency indicates positive attitudes from generalized residents toward that option, while lower frequency indicates negative attitudes. Considering the three variables differ in question content presentation, the questionnaire design includes questions with two-scale, three-scale, and five-scale options based on actual conditions, as shown in Table 1 . To comprehensively reveal coupling influence patterns of scenarios across different demographic groups, the questionnaire includes demographic questions on gender, age group, education level, community residence duration, and occupation.

Table 1 Core Question Design

Question Content and Options	Variable
Many vending machines now support "facial payment," allowing payment through facial recognition without mobile QR codes. Have you tried "facial payment"? [Single choice: A. Yes, B. Didn't know facial payment was available, C. No]	Self-interest
If property management distributes forms to every household to collect all residents' personal information including mobile numbers, ID numbers, and photos for strengthened community management, would you actively cooperate? [Single choice: A. Yes, B. No]	Altruism
Do you support community adoption of facial recognition access control systems for community gates and building unit doors? [Single choice: A. Support, B. Indifferent, C. Oppose]	Public-benefit
In recent years, China's public security system has vigorously promoted the "Xueliang Project," installing video surveillance in many public places. If traveling with minor children, would you hope the surveillance system could help prevent child loss? [Single choice: A. Very much hope, B. Somewhat hope, C. Indifferent, D. Somewhat don't hope, E. Very much don't hope]	Self-interest/Public-benefit*

Question Content and Options	Variable
When video surveillance systems in public places are used to find lost children, clear facial images of the child are needed for comparison. If you are the guardian (parent) of a minor child, under strict privacy protection measures, would you be willing to upload the child's facial recognition image to the system in advance before traveling for immediate search activation in case of child loss? [Single choice: A. Very willing, B. Somewhat willing, C. Indifferent, D. Somewhat unwilling, E. Very unwilling]	Self-interest/Public-benefit*

Note: Variables marked with are relative judgment values.

In data analysis, results from the three different scales need to be unified. For three-scale option questions, option B by default has half probability leaning toward option A's attitude and half toward option C's attitude, thus converted to two-scale results. Following the same logic, five-scale option question results can be converted to three-scale, then further to two-scale. Defining the personal information disclosure intention quantification indicator as $lg\omega$, ω is calculated as follows:

$$\omega = \begin{cases} \frac{r(A)+0.5r(B)}{r(C)+0.5r(B)}, & \text{Question numbers 01 and 02} \\ \frac{r(A)+0.75r(B)+0.5r(C)+0.25r(D)}{r(E)+0.75r(D)+0.5r(C)+0.25r(B)}, & \text{Question numbers 04 and 05} \end{cases}$$

where $r(i), i \in [A, B, C, D, E]$, represents the frequency of each option for that question, with values shown in Figure 3 [Figure 3: see original paper].

2.4 Questionnaire Distribution and Collection

This study utilized a professional questionnaire survey system starting from January 17, 2020, distributing and collecting questionnaires through 260 registered surveyors. To avoid potential impacts from national epidemic prevention and control work, data collection was cut off on February 8, 2021, obtaining 1,943 questionnaire responses from over 20 provinces and cities including Beijing, Henan, and Anhui. After eliminating incomplete and non-standard invalid questionnaires, 1,526 valid questionnaires were obtained with the following statistical characteristics: (1) near-equal gender ratio; (2) nearly 70% young people aged 18-30, with most respondents between 18-60, the age range concentrated with social activity participants and information technology users; (3) education levels ranging from junior high school and below to doctoral students, with higher education being predominant; (4) community residence duration ranging from new migrants within one year to long-term residents over ten years; (5) comprehensive occupational coverage. The valid respondents covered a wide

range, providing good universality and breadth of collected data, with specific results shown in Figure 2 [Figure 2: see original paper].

Statistical results for the five core questions in Table 1 from this survey are shown in Figure 3 [Figure 3: see original paper].

3 Impact of Scenarios on Disclosure Intention

3.1 Data Pattern Analysis

Calculating personal information disclosure intention across different interest tendency scenarios using formula (1) reveals regular differences in residents' willingness to disclose personal information. Disclosure intention is relatively low in self-interest scenarios and relatively high in public-benefit scenarios. Considering that question 01 might generate negative intention toward vending machine facial payment due to lack of access opportunity, question 06 was introduced: "Does your community have vending machines? [Options: A. Yes, B. No, C. Don't know]" as a constraint condition. Cross-tabulation with question 01 yielded corrected data shown in Table 2 . The corrected $lg\omega$ value calculated using data from communities with vending machines is 0.316, with comparison shown in Figure 4 [Figure 4: see original paper]. The comparison shows that although the corrected data shows higher intention than question 01, there is no qualitative change overall. Residents' personal information disclosure intention increases sequentially along self-interest, altruism, and public-benefit scenarios, maintaining the aforementioned result.

Table 2 Corrected Data for Question 01

Question 01	Question 06
A. Yes	A. Yes
B. No	B. No
C. Don't know	C. Don't know

Similarly, calculations for personal information disclosure intention across different security relevance scenarios are shown in Figure 5(a) [Figure 5: see original paper], and across different disclosure degrees in Figure 5(b) [Figure 5: see original paper]. Residents' personal information disclosure intention is positively correlated with scenario security relevance and negatively correlated with disclosure degree across scenarios. When personal information use scenarios involve higher public safety relevance, residents' disclosure intention increases accordingly. When scenarios involve higher personal information disclosure degree, residents' disclosure intention decreases accordingly, though the latter difference is not significant.

Figure 4 x_1 Personal Information Disclosure Intention

Figure 5 x_2, x_3 Personal Information Disclosure Intention

Clearly, the disclosure degree variable shows the lowest sensitivity in this survey, while the interest tendency variable has the most significant impact on personal information disclosure intention. That is, residents show significantly high willingness to disclose personal information in public-benefit and high-security-related scenarios. Integrating data from the five questions in order from public-benefit to altruism according to interest tendency yields results shown in Figure 6 [Figure 6: see original paper].

Figure 6 Multi-dimensional Integrated Distribution of Disclosure Intention

3.2 Discussion of Findings

Further analysis of the survey statistics suggests the following possible reasons:

(1) As an emerging practice, facial payment has not yet formed widespread usage habits. For most residents, although disclosing facial information for payment convenience is self-interested, the satisfied needs are largely non-essential, resulting in very limited perceived benefits. Therefore, in "non-essential self-interest" scenarios, residents' personal information disclosure intention is low.

(2) Under Chinese social culture, when facing public safety-related emergencies like infectious disease outbreaks that require personal information disclosure, there is often a phenomenon of expanded public power scope and relative reduction of individual rights. Residents generally show positive attitudes. In China's COVID-19 community prevention and control, residents widely recognized and complied with unified government epidemic prevention rules and procedures, actively monitoring epidemic situations and complying with community prevention requirements. This phenomenon of transforming personal information collection and other epidemic prevention policies into personal active responsibility aligns with OCB dimensions including organizational compliance, civic virtue, personal initiative, and self-development [35].

(3) As an organization, community governance shows significant OCB factor influence on personal information disclosure intention. According to C. Smith's earliest OCB classification [36], disclosing personal information includes at least altruism and generalized compliance dimensions. Mainstream views hold that citizen performance in social exchange theory forms the basis for generating altruism and generalized compliance mechanisms [37-38]. Residents' personal information disclosure behavior for community governance needs typically calculates potential returns in social relationships in more implicit ways. For example, most residents' willingness to accept and cooperate with identity verification at access control systems largely stems from obtaining shared returns through improved community order at acceptable costs.

4 Coupling Influence Patterns of Individual Attributes and Scenarios

4.1 Statistical Analysis of Individual Attributes from Questionnaires

Scenario variables may have differentiated influence patterns on personal information disclosure intention across different populations. Therefore, individual attribute variables are further superimposed for analysis. Since question 01 correction does not affect the analysis, simplified processing is applied.

First, based on the ologit model, data from questions 01-05 were regressed separately using four individual attributes from the questionnaire—gender, age group, education level, and community residence duration—as independent variables. The ologit model regression analysis results for gender, age group, education level, and community residence duration are shown in Table 3 .

Table 3 Ologit Model Regression Analysis

Variable	Question 01	Question 02	Question 03	Question 04	Question 05
Gender	0.353***	0.0774	-0.529***	-0.361***	-0.127
	(0.101)	(0.116)	(0.174)	(0.119)	(0.107)
Age Group	-0.179***	-0.0438	-0.0357	0.0925	0.0876
	(0.0570)	(0.0664)	(0.0959)	(0.0699)	(0.0622)
Education Level	0.0619	-0.102**	0.208***	-0.0239	0.0599
	(0.0433)	(0.0511)	(0.0702)	(0.0517)	(0.0469)
Community Residence Duration	-0.0272	-0.0123	0.172***	0.136***	0.173***
	(0.0362)	(0.0414)	(0.0607)	(0.0416)	(0.0377)
/cut1	-0.383	-1.464***	-2.093***	-5.306***	-4.067***
	(0.260)	(0.311)	(0.426)	(0.540)	(0.417)
/cut2	-0.102	—	-1.234***	-4.134***	-2.739***
	(0.260)		(0.418)	(0.393)	(0.319)
/cut3	—	—	—	-2.632***	-1.595***
				(0.326)	(0.290)
/cut4	—	—	—	-0.650**	0.396
				(0.309)	(0.282)
Observations	1,526	1,526	1,526	1,526	1,526

Standard errors: *** p<0.01, ** p<0.05, * p<0.1

For question 01, males show 35.3% higher intention than females, significant at the 1% level, indicating males are more inclined to use facial payment. Each age group level increase reduces intention probability by 17.9%, significant at the 1% level, showing facial payment intention decreases with age. Education level

and community residence duration did not pass significance tests, indicating these variables have no effect on facial payment intention.

For question 02, each education level increase reduces intention probability by 10.2%, significant at the 5% level, indicating higher-educated residents have lower intention to cooperate with property management's personal information collection. Gender, age group, and community residence duration did not pass significance tests, indicating these three variables have no effect on cooperation intention.

For question 03, females show 52.9% higher intention than males, significant at the 1% level, indicating females have higher intention for facial recognition access control systems. Each education level increase raises intention probability by 20.8%, significant at the 1% level, indicating higher-educated residents have higher intention for facial recognition access control systems. Each community residence duration level increase raises intention probability by 17.2%, significant at the 1% level, showing intention for facial recognition access control systems increases with community residence duration. Age group did not pass significance tests, indicating no effect on intention for facial recognition access control systems.

For question 04, females show 36.1% higher intention than males, significant at the 1% level, indicating females have higher acceptance of video surveillance systems collecting personal information. Each community residence duration level increase reduces intention probability by 13.6%, significant at the 1% level, showing acceptance of video surveillance systems decreases with community residence duration. Age group and education level did not pass significance tests, indicating these two variables have no effect on acceptance of video surveillance systems collecting personal information.

For question 05, each community residence duration level increase raises intention probability by 17.3%, significant at the 1% level, indicating residents' willingness to proactively provide facial recognition images for safety considerations increases with community residence duration. Gender, age group, and education level showed no significant differences for this question.

Second, since occupational variable values are independent discrete values, cross-tabulation analysis was used separately for occupation. Cross-tables were constructed with occupation as the filter condition, and $lg\omega$ values for personal information disclosure intention across different occupational categories were calculated row by row using formula (1), as shown in Table 4 . Comparison with overall experimental sample disclosure intention calculation results (Figure 6) is shown in Figure 7 [Figure 7: see original paper], where the horizontal axis represents the five questions, the vertical axis represents $lg\omega$ values, and line L_0 represents the overall experimental sample disclosure intention values.

Using L_0 data as the reference sequence and $L_i(i = 1, 2, ..., 10)$ data as observation sequences, SPSS was used to measure similarity distances between variables to quantify geometric shape similarity of the lines, as shown in Fig-

ure 8 [Figure 8: see original paper]. Among occupational categories, residents from foreign enterprises (L_5) and unemployed residents (L_6) show obvious differences in disclosure intention across scenarios compared to other occupations. Hourly/contract workers (L_7) show characteristics of higher self-interest scenario disclosure intention than altruism scenario for facial information. This further confirms that different scenarios can explain the influence mechanism on personal information disclosure intention.

Table 4 Personal Information Disclosure Intention Calculation Results by Occupation

Occupation	Q01	Q02	Q03	Q04	Q05
Government/Institutions	0.013	0.117	0.422	0.868	0.769
State-owned Enterprises	-0.053	0.473	0.681	1.201	1.028
Private Enterprises	-0.047	0.266	1.114	1.243	0.843
Foreign Enterprises	0.097	0.287	1.282	1.106	0.971
Unemployed	0.000	0.146	1.317	1.095	0.747
Students	-0.167	0.681	1.088	0.900	0.886
Hourly/Contract Workers	0.494	0.025	0.527	0.845	1.119
Retirees	0.147	0.462	0.681	1.013	1.294
Freelancers	-0.178	0.644	1.459	1.033	1.106
Other Institutions	0.238	0.845	1.144	1.074	1.101

Figure 7 Comparison of Personal Information Disclosure Intention by Occupation

Figure 8 Quantified Geometric Shape Similarity of Lines

4.2 Characteristic Discussion

The above analysis reveals that different individual attributes cause community residents' personal information disclosure intention to be differently affected by scenario variables. This provides guidance for communities to implement precise policies based on their characteristics and personal information application needs. The underlying causes of these differences are discussed below based on survey conditions and OCB theory:

Gender Factors: Analysis shows females exhibit more obvious OCB characteristics than males. In public-benefit scenarios, females show more positive attitudes toward disclosing personal information, while in self-interest scenarios, males are more willing to try benefits from emerging technologies. This result may synthesize gender differences in privacy concerns and organizational citizenship behavior. Comparatively, females have higher privacy security concerns than males [29-30, 39], but for females, prosocial value motivations are more important [40].

Age Group Factors: Analysis shows personal information disclosure intention decreases with age in non-essential self-interest scenarios but shows no obvious change in public-benefit and altruism scenarios. This result aligns with the general pattern that young people are more willing to try emerging technologies than older adults. It also indicates that in most public-benefit scenarios in community governance, attitudes toward personal information collection and use show no differential attitudes among residents of different ages.

Education Level Factors: Analysis shows higher education levels lead to more cautious attitudes toward personal information disclosure in altruism scenarios but more positive attitudes in access control systems with mixed self-interest and public-benefit tendencies. This means higher-educated community residents pay more attention to information recipients, information purposes, and necessity regarding personal information collection and use.

Community Residence Duration Factors: Analysis shows longer fixed residence duration in communities leads to higher personal information disclosure intention in public-benefit scenarios with self-interest tendencies. This indicates that more stable residential status leads to stronger potential pursuit of personalized self-interest needs in community governance-oriented personal information disclosure processes and possibly higher OCB tendencies. This result confirms D. Organ's view that "OCB accumulates gradually over time" [41].

Occupation Factors: Analysis shows different occupational categories yield differentiated results for personal information disclosure intention across scenarios. Foreign enterprise employees, unemployed residents, and hourly/contract workers show obvious differences from other occupations, warranting further in-depth investigation into their underlying reasons or mechanisms.

5 Conclusions and Implications

5.1 Conclusions and Theoretical Contributions

Since no risk evolution process can avoid human factors, and communities serve as outposts for risk perception monitoring, prediction, warning, and intelligent prevention [42], collecting and using personal information is essential for community governance including epidemic prevention and control. Personal information application depends on harmonious "disclosure-collection" relationships. Exploring strategies for personal information application that align with residents' disclosure intention is a key prerequisite for implementing diversified and precise individual risk governance and demand services within jurisdictions, significantly impacting the implementation of a co-construction, co-governance, and shared community governance framework. This study's comprehensive analysis of influence patterns of scenarios and individual attributes on community residents' personal information disclosure intention has important theoretical and practical value for optimizing data-driven community governance strategies. Conclusions are summarized as follows:

(1) Among the three sets of scenario variables, interest tendency and security relevance significantly affect residents' personal information disclosure intention. When setting scenarios for personal information application in community governance, focus should be placed on interest tendency and security relevance aspects.

(2) Appropriately introducing personalized services has certain significance for improving community residents' attitudes toward disclosing personal information, but satisfying non-essential needs has no actual effect on residents' attitudes.

(3) Residents show relatively high willingness to disclose personal information in public-benefit and safety-related scenarios. During community governance, needs for collecting personal information related to public interest and public safety protection are more likely to gain residents' recognition and acceptance.

(4) Individual attributes including gender, age group, education level, community residence duration, and occupation have certain influences on how scenarios affect disclosure intention. Personal information application strategies for community governance need to consider the distribution characteristics of different individual attributes among community residents.

Additionally, this study introduces OCB theory to reveal how community governance personal information application scenarios influence residents' personal information disclosure intention, supplementing and enriching theoretical foundations for building multi-stakeholder collaborative governance organizations around personal information application in the big data era. Research shows residents' willingness to disclose personal information for community governance demonstrates obvious OCB characteristics. Therefore, incorporating residents into the community governance organizational system and optimizing scenarios helps stimulate residents' OCB, which is significant for building harmonious personal information "disclosure-collection" relationships and promoting precise community governance.

5.2 Implications and Research Outlook

Under the premise of privacy protection, this study provides the following insights for building personal information application scenarios that align with residents' willingness and exploring more reasonable community personal information collection and use models:

(1) Emphasizing public safety protection as the main task and key approach in community governance, highlighting the "public-benefit" tendency of personal information collection and use scenarios, helps obtain more positive personal information disclosure intention from community residents. Simultaneously, introducing necessary information technology to replace manual processes with public information channels reduces community

governance staff's personal behaviors, thereby highlighting the public nature of personal information application, which is also crucial for obtaining trustworthy and effective personal information support for community governance.

(2) Changing the motivation for personal information application in community governance, truly following the "people-centered" principle, fully considering and responding to residents' actual personalized needs. Particularly in community announcements and work interactions, residents' interests should be prioritized. It must be clear that personal information collection and use serve residents themselves rather than directly facilitating community governance work. For example, during epidemic prevention and control, community personnel screening information not only satisfies population flow management but more importantly enables precise centralized material supply and basic living support, thereby achieving "feedback" balance from community governance to individual residents through personal information.

(3) Personal information application strategies in community governance should adapt to local conditions. Particularly for communities with obvious resident individual attribute distribution characteristics such as youth communities (talent apartments), elderly communities, university communities, and rural communities, personalized solutions adapted to community realities should be formulated. This should both targetedly stimulate and amplify OCB among different resident groups and fully respond to community residents' concerns about personal information collection and use.

(4) Extending from community governance personal information disclosure issues, residents are proper roles in the community governance organizational system. Effectively advancing the co-construction, co-governance, and shared community governance framework means transforming residents from single governance objects to organizational members participating in governance. We should fully explore and guide OCB driven by social responsibility, guiding residents to recognize that reasonable personal information disclosure contributes to "co-constructing" community governance big data resources, represents the most direct action in participating in community governance "co-governance," and enables "sharing" harmonious and orderly community safety guarantees, thereby effectively improving residents' responsive attitudes toward various cooperative affairs and ultimately enhancing overall community governance organizational performance.

This study has some limitations that can guide future research directions. On one hand, the study uses non-scale questionnaire data to reveal OCB phenomena in residents' personal information disclosure for community governance from scenario and individual attribute perspectives, while neglecting quantitative research on OCB generation mechanisms. Future research could attempt to de-

velop specialized OCB scales to further reveal OCB degrees presented by different community residents and different personal information application scenarios. On the other hand, this study treats privacy protection as a constant, omitting the influence of different privacy security conditions. However, issues such as technical anonymization failures [6] mean we cannot currently achieve essential security of personal information. Privacy security level is inevitably a main variable affecting personal information disclosure intention. Future research could integrate numerous research findings on privacy security and personal information disclosure to discuss coupling influence mechanisms of more factors.

References

[1] KISSLER S M, TEDIJANTO C, GOLDSTEIN E, et al. Projecting the transmission dynamics of SARS-CoV-2 through the pandemic period [J]. Science, 2020, 368(6493): 860-868.

[2] Ministry of Civil Affairs, National Health Commission. Notice on Issuing the "Guidance Plan for Precise and Refined Community Prevention and Control and Service Work for COVID-19" (Minfa [2020] No. 38) [EB/OL]. [2021-07-07]. http://www.gov.cn/zhengce/zhengceku/2020-04/16/content_{5503261}.htm.

[3] ZHANG Y D, WANG Q, LIU Y. Personal data application in community governance in the "post-pandemic era": Problems and strategies [J]. E-Government, 2021(2): 84-96.

[4] FAHEY R A, HINO A. COVID-19, digital privacy, and the social limits of data-focused public health responses [J]. International Journal of Information Management, 2020, 55: 102181.

[5] PAN X B. Application of personal-oriented digital technology in preventing transmission of COVID-19, China [J]. Irish Journal of Medical Science, 2020, 189(4): 1-2.

[6] OHM P. Broken promises of privacy: Responding to the surprising failure of anonymization [J]. UCLA Law Review, 2010, 57: 1701-1777.

[7] MAI J E. Big data privacy: The datafication of personal information [J]. The Information Society, 2016, 32(3): 192-199.

[8] ZHAROVA A K, ELIN V M. The use of big data: A Russian perspective [J]. Computer Law & Security Review, 2017, 33(4): 482-501.

[9] STOUGH R, MCBRIDE D. Big data and U.S. public policy [J]. Review of Policy Research, 2014, 31(4): 339-342.

[10] TENE O, POLONETSKY J. Privacy in the age of big data: A time for big decisions [J]. Stanford Law Review Online, 2012, 64(63): 63.

[11] BANSAL G, ZAHEDI F M, GEFEN D. Do context and personality matter? Trust and privacy concerns in disclosing private information online [J].

Information & Management, 2016, 53(1): 1-21.

[12] WANG L, YAN J, LIN J, et al. Let the user tell the truth: Self-disclosure intention and self-disclosure honesty in mobile social networking [J]. International Journal of Information Management, 2017, 37(1): 1428-1440.

[13] LIU Z, WANG X. How to regulate individuals' privacy boundaries on social network sites: A cross-cultural comparison [J]. Information & Management, 2018, 55(8): 1005-1023.

[14] GOPAL R D, HIDAJI H, PATTERSON R A, et al. How much to share with third parties? User privacy concerns and website dilemmas [J]. MIS Quarterly, 2018, 42(1): 143-164.

[15] 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, 51(1): 42-52.

[16] MEI X. The legal attributes of electronic data and the positioning of data in civil law [J]. Social Sciences in China, 2019, 40(1): 82-92.

[17] CHENG X. Personal data rights in the era of big data [J]. Social Sciences in China, 2019, 40(3): 174-188.

[18] KIM J K, KIM S H. Intention to disclose personal information in LBS: Based on privacy calculus perspective [J]. Journal of Information Systems, 2012, 21(4): 55-79.

[19] TREIBLMAIER H, CHONG S. Trust and perceived risk of personal information as antecedents of online information disclosure: Results from three countries [J]. Journal of Global Information Management, 2011, 19(4): 76-94.

[20] CHELLAPPA R K, SIN R G. Personalization versus privacy: An empirical examination of the online consumer's dilemma [J]. Information Technology & Management, 2005, 6(2/3): 181-202.

[21] KIM D, PARK K, PARK Y, et al. Willingness to provide personal information: Perspective of privacy calculus in IoT services [J]. Computers in Human Behavior, 2019, 92(3): 273-281.

[22] YEH C H, WANG Y S, LIN S J, et al. What drives internet users' willingness to provide personal information? [J]. Online Information Review, 2018, 42(6): 923-939.

[23] LIU Z L, HUANG J H. Review of information privacy research and development [J]. Information Science, 2012, 30(8): 1258-1262.

[24] ROBINSON C. Disclosure of personal data in e-commerce: A cross-national comparison of Estonia and the United States [J]. Telematics & Informatics, 2017, 34(2): 569-582.

[25] WANG L, WANG L Y, SUN Z. Influence mechanism of privacy violation experience on online users' self-disclosure [J]. Systems Engineering—Theory &

Practice, 2020, 40(1): 79-92.

[26] XU H, DINEV T, SMITH H J, et al. Information privacy concerns: Linking individual perceptions with institutional privacy assurances [J]. Journal of the Association for Information Systems, 2011, 12(12): 798-824.

[27] LIU Z, WANG X. How to regulate individuals' privacy boundaries on social network sites: A cross-cultural comparison [J]. Information & Management, 2018, 55(8): 1005-1023.

[28] BELLAAN S, JOHNSON E J, KOBRIN S J, et al. International differences in information privacy concerns: A global survey of consumers [J]. Information Society, 2004, 20(5): 313-324.

[29] FAJAS S, TRIMIS S. Privacy concerns in e-commerce: An empirical investigation of gender differences [J]. International Journal of Electronic Business, 2008, 6(4): 386-404.

[30] SHEEHAN K B. An investigation of gender differences in online privacy concerns and resultant behaviors [J]. Journal of Interactive Marketing, 1999, 13(4): 24-38.

[31] KEHR F, WENTZEL D, MAYER P. Rethinking the privacy calculus: On the role of dispositional factors and affect [C]//Thirty Fourth International Conference on Information Systems (ICIS 2013). Milan: AISeLibrary, 2013: 1-10.

[32] LI Y P, TU Y D. Research on the value orientation of organizational citizenship behavior [J]. Management World, 2012(5): 1-7, 61.

[33] ZHANG X L, QI Z J. Organizational citizenship behavior theory and its application research [J]. Advances in Psychological Science, 2001, 9(4): 352-360.

[34] WHITE M E. Training and educating army officers for the 21st century: Implications for the United States Military Academy [R]. Fort Belvoir: Defense Technical Information Center, 1998.

[35] PODSAKOFF P M, MACKENZIE S B, PAINE J B, et al. Organizational citizenship behaviors: A critical review of the theoretical and future research [J]. Journal of Management, 2015, 26(3): 513-563.

[36] SMITH C A, ORGAN D W, NEAR J P. Organizational citizenship behavior: Its nature and antecedents [J]. Journal of Applied Psychology, 1983, 68(4): 653-663.

[37] KELLY L Z, BENNETT J T. Beyond social exchange: New directions for organizational citizenship behavior theory and research [J]. Research in Personnel & Human Resources Management, 2003, 22(3): 395-424.

[38] SHENG L F, SHI Z L. Generation mechanism and induction strategies of organizational citizenship behavior [J]. Journal of Beijing Jiaotong University (Social Sciences Edition), 2009, 8(3): 64-68.

[39] ROWAN M, DEHLINGER J. Observed gender differences in privacy concerns and behaviors of mobile device end users [J]. Procedia Computer Science, 2014, 37: 340-347.

[40] DÁVILA C, FINKELSTEIN M A, CASTIÉN J I. Gender differences in prosocial behavior: Organizational citizenship behavior [J]. Anales de Psicología, 2011, 27(2): 498-506.

[41] ORGAN D W. Organizational citizenship behavior: The good soldier syndrome [M]. Lexington: Lexington Books, 1988.

[42] SU A P. Taking multiple measures to promote precise community governance [N]. Economic Daily, 2020-08-12(11).

Author Contributions: Zhang Yudong: Proposed the overall research framework and wrote the paper; Wang Qi: Data analysis and preprocessing; Qian Jing: Questionnaire survey; Liu Yi: Determined the research topic and revised the paper.

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