Research on the Formation Mechanisms of User Privacy Paradox in the Context of Quantified Self

Authors: Shanji Yao, Wenli Liu, Liu Jiajing, Yao Shanji

Date: 2025-11-05T18:35:54+00:00

Abstract

[Purpose/Significance] Exploring the privacy paradox phenomenon in the context of quantified self contributes to resolving the dilemma of personal information protection, promoting standardized management of health management platforms, and providing theoretical basis and practical reference for positive interaction between platforms and users. [Method/Process] First, user data were collected through interviews and subjected to three-level coding using procedural grounded theory; second, a theoretical model of the privacy paradox formation mechanism was constructed by combining qualitative research findings with existing literature; finally, empirical testing was conducted based on data from 309 questionnaires. [Results/Conclusion] Users' perceived severity and perceived susceptibility enhance privacy concerns and reduce privacy disclosure intention; privacy concerns also reduce privacy disclosure intention and mediate the relationship between perceived severity and privacy disclosure intention. Both technological affordance and boundary management can weaken or even reverse the negative effect of privacy concerns on privacy disclosure intention, and also attenuate the negative mediating role of privacy concerns between perceived severity and privacy disclosure intention.

Full Text

Preamble

Research on the Formation Mechanism of User Privacy Paradox in the Context of Quantified Self

Yao Shanji*, Liu Wenli, Liu Jiajing
School of Economics and Management, Nanjing Tech University, Nanjing 211816, China

Abstract:
[Purpose/Significance] This study explores the privacy paradox phenomenon

in the context of quantified self, providing theoretical and practical insights to address challenges in personal information protection, promote standardized management of health management platforms, and foster positive interactions between platforms and users. [Method/Process] First, user data were collected through interviews and analyzed using procedural grounded theory with three-stage coding. Then, integrating the qualitative findings with existing literature, a theoretical model of the privacy paradox formation mechanism was constructed. Finally, an empirical test was conducted using data from 309 valid questionnaires. [Result/Conclusion] Users' perceived severity and perceived susceptibility enhance privacy concerns and reduce privacy disclosure intention. Privacy concern also reduces privacy disclosure intention and mediates the relationship between perceived severity and privacy disclosure intention. Both technological affordance and boundary management can mitigate or even reverse the negative effect of privacy concern on privacy disclosure intention, as well as weaken the mediating role of privacy concern between perceived severity and privacy disclosure intention.

Keywords: Quantified self; Privacy paradox; Privacy disclosure intention; Privacy concern; Smart wearable devices; Online health

The "Healthy China" strategy prioritizes people' s health as a strategic development priority, with the "Healthy China Action (2019-2030)" further clarifying that every individual is the first responsible person for their own health, providing a concrete pathway for strategy implementation. In this context, how to scientifically and effectively manage personal health has become an important public concern, and quantified self offers an effective approach for individuals to achieve health management goals. Through quantified self devices or applications, users can track and record their health status and behavioral habits in real time. With the rapid development of information technology, quantified self has evolved into an emerging lifestyle that has permeated healthcare, education, consumption, and other fields [1]. In recent years, the proliferation of smart wearable devices and online health applications has further propelled the development of quantified self, focusing increasingly on the quantified management of personal health data and becoming an emerging domain of health information management [2].

User privacy disclosure constitutes the prerequisite and foundation of quantified self. Service providers collect, store, and analyze large amounts of user personal information to deliver health information services, while users provide this information to obtain corresponding services [3]. In this interactive process, a notable phenomenon emerges: users are concerned about personal privacy information being leaked and misused, yet they choose to disclose privacy information to service providers [4]. This phenomenon, where users express privacy concerns attitudinally while disclosing privacy behaviorally, is termed the privacy paradox [5]. Currently, privacy paradox research predominantly focuses on contexts such as social media and online shopping [6-7], with relevant explorations for quantified self not only extremely scarce but also methodologically

limited. Moreover, academic consensus on whether the privacy paradox exists remains unachieved [8]. Some studies confirm the existence of the privacy paradox [9-10], while others indicate its absence [11], suggesting that the privacy paradox may have certain boundary conditions [12]. Therefore, flexibly applying different research methods across different contexts helps deepen understanding of the privacy paradox' s boundaries and better explain and address it.

This study aims to analyze the relationship between user privacy concerns and privacy disclosure intention in the quantified self context and explore the formation mechanism of the privacy paradox. Given that mixed methods can integrate the advantages of qualitative and quantitative research [13], this study adopts a logic of qualitative exploration followed by quantitative validation. First, qualitative data were collected through focus group interviews and in-depth interviews, using procedural grounded theory to excavate the influencing factors and formation mechanisms of the privacy paradox in the quantified self context. Second, based on qualitative findings and existing literature, a theoretical model of the privacy paradox formation mechanism was constructed, and data were collected through questionnaires for empirical testing. This study can provide practical insights for user privacy information management and sustainable development in the health service domain, as well as theoretical references for research deepening in health information management in the digital intelligence era.

2.1 Quantified Self

Quantified self originally referred primarily to individuals' continuous tracking and analysis of personal data [14]. Quantified self is the result of self-tracking [15], with some studies also using self-tracking to represent quantified self [16]. Definitions of quantified self remain inconsistent. K. Maltseva et al. define quantified self as the process of collecting and reflecting on personal data through wearable devices and self-tracking applications [15]; Feng Shan et al. consider quantified self as a process of exploring and reflecting on personal quantified data to obtain self-awareness [17]; D. Lupton summarizes quantified self as using digital tools to track and measure health or behavior for self-improvement [18]. In short, quantified self is the process of using smart devices to monitor and manage personal data, driven by data, mediated by quantified devices, and goal-oriented [1].

Quantified self has narrow and broad definitions. The former focuses primarily on the health domain, emphasizing data monitoring and analysis related to personal physiological activities and states, such as physical function and disease diagnosis data [2]. The latter is not limited to the health domain but encompasses individual cognition and behavior, such as time allocation and daily habits data [19]. With the rapid development of smart wearable devices and online health applications, quantified self is increasingly understood as the quantification of health data [2].

Since quantified self is based on user privacy information [4], privacy security issues have gradually attracted academic attention. If users refuse to provide privacy information to service providers, they cannot enjoy quantified services. Therefore, privacy disclosure is the focus of quantified self privacy research [20]. Existing research primarily explores privacy disclosure intention and behavior in quantified self from perspectives such as privacy calculus theory, communication privacy management theory, elaboration likelihood model, and affordance theory, revealing users' privacy disclosure decision-making basis, boundaries, paths, and outcomes [1]. However, quantified self is still in its early development stage, with existing research mainly focusing on privacy disclosure while lacking exploration of other privacy-related issues such as the privacy paradox, requiring further deepening and expansion.

2.2 Privacy Paradox

S. B. Barnes first proposed the privacy paradox, with subsequent scholars providing clear definitions [21]. For example, M. C. Oetzel et al. refer to the discrepancy between individuals' subjective concerns about privacy threats and actual privacy disclosure behavior as the privacy paradox [5], while T. Dienlin et al. directly define it as the lack of association between individuals' privacy concerns and privacy behaviors [11]. Despite definitional variations, they essentially reflect the phenomenon where users worry about privacy security yet disclose privacy.

Current privacy paradox research primarily concentrates on scenarios such as social media [6], online shopping [7], online health communities [22], and smart applications [23], generally based on perspectives like privacy calculus theory, construal level theory, and regulatory focus theory. Influencing factors and formation mechanisms are research priorities. Regarding influencing factors, existing research generally categorizes them into four aspects: cognitive, psychological, need-based, and environmental [8]. Cognitive factors mainly include perceived benefits, perceived risks, and self-efficacy [7, 24]; psychological factors involve privacy concerns [25]; need-based factors manifest as personalized needs and social needs [8]; environmental factors encompass social norms and collectivist tendencies [6, 25]. Regarding formation mechanisms, research typically explores internal and external aspects. Internal causes mainly include rational and irrational privacy calculus processes, with the former based on weighing privacy risks and benefits and the latter manifesting as bounded rationality and cognitive biases [4]; external causes focus on external factors such as social norms [8].

However, as a contradictory phenomenon, academic consensus on the privacy paradox' s existence remains debated [8]. Some studies confirm the privacy paradox in social media [26], online healthcare [9], and online shopping contexts [10], while others indicate its absence [12]. For example, T. Dienlin et al. note that under new methodological applications, social network users' privacy concerns indirectly reduce privacy disclosure behavior through privacy attitudes

and intentions [11]. This suggests the privacy paradox phenomenon may have boundary conditions related to research context, mediating variables, platform types, and survey subjects [12].

2.3 Summary

Based on the above literature review, quantified self has attracted widespread academic attention, with its core lying in continuously collecting and analyzing personal health data through digital intelligence tools. Particularly, as such data directly reflects personal physical health status and is highly sensitive, users' privacy security concerns are often stronger. However, to obtain personalized health management services, users still choose to disclose privacy, constituting a typical privacy paradox phenomenon. Furthermore, compared to contexts like social media, the health data involved in quantified self, due to its high sensitivity, easily triggers higher levels of privacy concerns, making the privacy paradox contradiction more complex in this context. Therefore, conducting privacy paradox research in quantified self not only helps deeply understand users' complex privacy behaviors but also promotes positive user-platform interactions to drive sustainable development of health information management platforms. However, existing literature mostly focuses on quantified self users'privacy disclosure, with relatively little attention to the contradictory phenomenon of the privacy paradox. Moreover, current privacy paradox research mainly concentrates on social media and online shopping contexts and has not reached consistent conclusions, suggesting the privacy paradox may have specific boundary conditions, making exploration of its formation mechanism in the quantified self context more valuable. More critically, most studies tend to use single methods to explore the privacy paradox formation, lacking systematic and comprehensive investigation of this contradictory phenomenon, urgently requiring breakthroughs.

3.1 Qualitative Data Collection

This study collected qualitative data using a combination of focus group interviews and in-depth interviews conducted in January 2025. According to Xu Xiaoting et al. [27], quantified self participants are primarily young and middle-aged adults who typically have strong health management motivations and relatively high acceptance and usage intentions for health management technologies. Therefore, this study targeted young and middle-aged groups as primary respondents, defined as users who had continuously used smart wearable devices or online health applications for at least one month, while striving to balance differences in age, gender, and occupation to improve sample representativeness. The study ultimately interviewed 23 users, including 15 semi-structured interviewees with a total interview time of approximately 432 minutes, and one focus group of 8 people with an interview time of approximately 60 minutes. Interviewee basic information is shown in Table 1 .

Before formal interviews, interviewers briefly stated interview rules and

promised data confidentiality. Each respondent received 50 RMB compensation after the interview. The interview outline mainly included questions such as "Are you concerned about privacy issues?" , "What are your reasons for being concerned or not concerned?" , and "What are your reasons for choosing to disclose privacy to service providers?"

3.2 Qualitative Data Analysis

This study adopted the procedural grounded theory method because it constructs theory inductively, making it suitable for exploring individuals' cognition, feelings, and interpretations of the external world [28-29], aligning with the research question. Additionally, this method is appropriate for studying complex social phenomena and is highly sensitive to context [28], while the privacy paradox phenomenon in the quantified self context has not yet been systematically and comprehensively studied, making this method suitable for exploration. Therefore, this study used NVivo20 software, following procedural grounded theory steps to conduct open coding, axial coding, and selective coding on interview texts to explore privacy paradox influencing factors. Before formal coding, considering theoretical saturation for theory construction and referencing Li Caining et al. [30], Excel' s random function was used to select 1/4 of interview samples (6 people) for theoretical saturation testing.

(1) Open Coding

The open coding stage aimed to obtain initial concepts and sub-categories. This process was completed jointly by two researchers in a "back-to-back" manner through keyword extraction, labeling, conceptualization, and categorization. During analysis and induction of interview texts, researchers found the initial concepts were numerous and had some overlap, so they integrated these similar or overlapping concepts, ultimately obtaining 99 initial concepts. Subsequently, categorization was performed, continuing to summarize and name initial concepts belonging to the same category, resulting in 22 sub-categories. The concept extraction process is exemplified in Table 2 .

(2) Axial Coding

Axial coding aims to identify and clarify relationships and contexts among subcategories, condensing sub-categories into main categories through further induction and clustering. After comprehensive comparative analysis and joint discussion of sub-categories, researchers ultimately condensed the 22 sub-categories obtained in the open coding stage into 6 main categories (B1-B6): perceived severity, perceived susceptibility, privacy concern, technological affordance, boundary management, and privacy disclosure intention. The category development process is shown in Table 3 .

(3) Selective Coding and Saturation Testing

Selective coding further integrates and refines based on axial coding, clarifying the core category and its logical relationships with other categories. Through in-depth analysis, this study identified the privacy paradox as the core category.

The main category relationship structure built around this core category is shown in Table 4 . Subsequently, the reserved 6 interview texts underwent the same coding analysis steps for theoretical saturation testing, with no new important concepts or relationship structures emerging, thus determining that coding results reached theoretical saturation.

3.3 Qualitative Research Results

The qualitative research identified six main categories: perceived severity, perceived susceptibility, privacy concern, technological affordance, boundary management, and privacy disclosure intention. Although existing literature was referenced during main category naming to enhance theoretical clarity, these main categories were formed based on systematic coding and gradual induction of interview materials. The interaction and dynamic relationships among these six main categories constitute the privacy paradox formation mechanism. First, when quantified self users use relevant devices or applications, they develop perceptions of privacy threats based on privacy security assessments, specifically manifested as judgments about the likelihood and severity of threat occurrence. This cognitive process is key to triggering privacy concerns and reducing privacy disclosure intention. As perceived threats increase, users' privacy security concerns strengthen, thereby inhibiting privacy disclosure intention. However, the relationship between privacy concern and privacy disclosure intention is not static; it is dynamically influenced by two moderating mechanisms: technological affordance and boundary management. On one hand, technological affordance provides possibilities for users to achieve quantified self goals, and users may still disclose privacy based on functional demands even when concerned. On the other hand, boundary management endows users with a certain degree of privacy control, making them willing to disclose privacy under conditions such as adjusting privacy settings. It is in this dynamic trade-off that the privacy paradox manifests.

However, although the relationship structure constructed by qualitative research initially received support from existing literature, this study conducted contextual expansion and theoretical extension based on existing literature, still requiring verification through empirical research. In other words, although qualitative research identified influencing factors of the privacy paradox in the quantified self context and preliminarily summarized its possible formation mechanisms, it could not quantify specific relationships among categories due to inherent limitations of qualitative methods. Therefore, this study subsequently conducted quantitative research.

4.1 Hypothesis Development

(1) Direct and Mediating Effect Hypotheses

Privacy concern refers to users' attention and worry about the security of privacy information provided to service providers [34]. Privacy disclosure intention

refers to users' willingness to disclose personal privacy information to service providers when using quantified self devices. The willingness to provide privacy information is closely related to concerns about privacy information security. However, research conclusions on their relationship have not yet reached consensus, showing significant differences across contexts and boundary conditions [8]. Some studies indicate privacy concern inhibits users'privacy disclosure intention [12], while others find privacy concern positively affects privacy disclosure intention, presenting the privacy paradox phenomenon [33]. Although this study focuses on the privacy paradox, interview findings revealed that users' privacy disclosure intention is generally low when they worry about privacy security, so this study still believes privacy concern negatively affects privacy disclosure intention in the quantified self context, though some boundary conditions may facilitate privacy paradox formation. Therefore, this study proposes that since using quantified self services requires disclosing sensitive information such as health or physical fitness, users concerned about privacy information security tend to reduce information disclosure to service providers [32].

Perceived severity refers to users' perception of the severity of potential consequences from privacy threats, focusing on how serious the consequences of privacy threats would be, while perceived susceptibility refers to users' perception of the likelihood of privacy threats occurring, focusing on how probable privacy threats are [35]. In the quantified self context, privacy disclosure as a prerequisite for obtaining quantified self services undoubtedly accompanies threats and risks of privacy leakage and misuse. According to protection motivation theory, users' assessment of privacy threats and risks affects their subsequent protective attitudes and behaviors. As two dimensions of threat assessment, both perceived severity and perceived susceptibility negatively affect privacy disclosure intention [36]. In the quantified self context, if users perceive that the leakage of privacy information provided to obtain quantified services would cause serious harm and high leakage risk, they will choose to reduce privacy information disclosure to minimize negative impacts and possibilities [31]. Based on the above, this study proposes:

H1: Privacy concern negatively affects privacy disclosure intention
H2: Perceived severity negatively affects privacy disclosure intention
H3: Perceived susceptibility negatively affects privacy disclosure intention

Since service providers' use of user information involves uncertainty and opportunistic tendencies, users typically experience some degree of privacy concern when providing privacy information to service providers [34]. Users'negative perceptions of privacy threats and risks are more likely to trigger privacy concerns [31]. Specifically, when users perceive high likelihood of privacy leakage and serious consequences of privacy leakage, they become more concerned about their privacy information security. Protection motivation theory states that besides privacy threat assessment, fear aroused by threat assessment is also crucial for users' privacy behavior and decision-making [36]. Further, assessment of privacy threat severity and susceptibility arouses users' privacy concerns, thereby affect-

ing their privacy disclosure decisions. Existing research indicates that users' perception processes of privacy threat severity and susceptibility also awaken users' privacy concerns, prompting them to pay more attention to privacy security protection and reduce privacy information disclosure [37]. Based on this, this study proposes:

H4a: Perceived severity positively affects privacy concern
H4b: Privacy concern mediates the relationship between perceived severity and privacy disclosure intention
H5a: Perceived susceptibility positively affects privacy concern
H5b: Privacy concern mediates the relationship between perceived susceptibility and privacy disclosure intention

(2) Moderating Effect Hypotheses

Users' privacy decisions are influenced not only by their subjective perceptions of privacy threats but also by technical environment and individual privacy control capabilities. As two important aspects of privacy decisions, boundary management and technological affordance represent users' privacy decision boundaries and outcomes, respectively, playing important roles in users' privacy behavior [1]. Existing research based on communication privacy management theory and affordance perspectives explores how service providers promote user information disclosure under reasonable and legal premises through functional design [38]. Some studies also note that boundary management and platform technological affordance interact to jointly influence user privacy decisions [39]. Therefore, incorporating affordance and boundary management into the same research framework helps comprehensively understand user privacy decisions.

Affordance originates from ecological psychology, referring to the possibilities that objective environments provide for individual action [40]. In information resource management, affordance is typically used to explore the potential possibilities that emerging technologies and digital tools bring for users to achieve goals [41]. Technological affordance is the most widely studied and applied affordance, emphasizing interaction between technology and users [42], specifically manifested as possibilities arising from interaction between behavioral and technical subjects, though these possibilities do not necessarily support behavioral subjects' goals [41]. Technological affordance varies by specific context and interaction method [43].

In the quantified self context, users need to provide personal information to service providers to achieve their goals, while service providers rely on processing this information to help users achieve goals, forming specific technological affordance. Privacy disclosure can be viewed as an interaction method between users and quantified self devices. At this time, technological affordance involves not only what quantified self devices can help users achieve but also the possible results of users disclosing privacy information to quantified self devices [44]. When users find that technological affordance helps achieve their goals, their privacy disclosure intention increases accordingly, and the degree of privacy disclosure depends on the strength of technological affordance [4]. Combined

with qualitative research, this study believes that users' privacy disclosure intention typically decreases under privacy concern, but technological affordance may change this situation. When users develop privacy concerns due to perceptions of privacy threat severity and susceptibility, they usually tend to refuse privacy disclosure. However, under technological affordance influence, if users realize that disclosing privacy information can achieve quantified self goals, their lower privacy disclosure intention will be improved. Therefore, this study proposes:

H6a: Technological affordance moderates the relationship between privacy concern and privacy disclosure intention
H6b: Technological affordance moderates the mediating effect of privacy concern between perceived severity and privacy disclosure intention
H6c: Technological affordance moderates the mediating effect of privacy concern between perceived susceptibility and privacy disclosure intention

Privacy boundary refers to the privacy range that users can control, i.e., the boundary between public and private information [45]. Different users have different privacy boundaries, varying in openness and thickness [1]. The same user also has different privacy boundaries when using different smart devices. Privacy boundaries are dynamically changing, and users can conduct boundary management according to personal needs and environmental rules. Users are more willing to disclose privacy information when they have effective boundary management authority [46]. Existing research shows that boundary management moderates the relationship between privacy concern and privacy disclosure intention in social media [33]. If users cannot effectively participate in privacy control while experiencing privacy concern, i.e., boundary management is chaotic, their privacy disclosure intention will significantly decrease, and they may even stop using the service [47]. When users are concerned due to perceptions of privacy threat severity and susceptibility, if they possess privacy control authority, the negative effect of privacy concern on privacy disclosure intention will be weakened, prompting them to use relevant devices or applications to track their health [48]. Therefore, this study proposes:

H7a: Boundary management moderates the relationship between privacy concern and privacy disclosure intention
H7b: Boundary management moderates the mediating effect of privacy concern between perceived severity and privacy disclosure intention
H7c: Boundary management moderates the mediating effect of privacy concern between perceived susceptibility and privacy disclosure intention

In summary, this study constructs a theoretical model of the formation mechanism of the privacy paradox for quantified self users, as shown in Figure 1 [Figure 1: see original paper].

4.2 Questionnaire Design and Data Collection

(1) Questionnaire Design
The questionnaire includes demographic information and measurement scales.

All scales were adapted from mature domestic and international scales and adjusted according to research content. Specifically, perceived severity measurement referenced Wang Luyao et al. [49] with 3 items; perceived susceptibility borrowed N. Mohamed et al.'s [50] scale with 3 items; privacy concern referenced T. Dinev et al.'s [34] scale with 3 items; technological affordance referenced Dong Xueyan et al. [51] with 5 items; boundary management referenced Xue Ke et al. [33] and H. Xu et al. [52] with 4 items; privacy disclosure intention referenced X. Cheng et al. [53] with 3 items. All variables were measured using a 7-point Likert scale (1 = strongly disagree, 7 = strongly agree).

(2) Data Collection

This study targeted users of quantified self devices or applications and collected data through the professional data research platform Credamo. To encourage participation, an incentive of 2 RMB was provided to each valid respondent. The questionnaire was distributed on February 3, 2025, with 350 copies issued. After excluding invalid questionnaires with missing answers, identical options, or regular patterns, 309 valid questionnaires were recovered, with an effective recovery rate of 88.3%. Sample distribution characteristics are shown in Table 5 .

(3) Reliability and Validity Analysis

Reliability and validity analysis is shown in Table 6 . All variables' Cronbach' s Alpha (CA) and Composite Reliability (CR) were above 0.7, indicating good scale reliability. All variables' factor loadings were greater than 0.6, and Average Variance Extracted (AVE) was greater than 0.5, indicating good convergent validity. Discriminant validity analysis is shown in Table 7 , where each variable' s AVE square root was greater than its correlation coefficients with other variables, indicating good discriminant validity. Additionally, the six-factor model comprising all variables showed acceptable fit indices (^{2}/df = 1.935, CFI = 0.952, TLI = 0.942, SRMR = 0.045, RMSEA = 0.055), indicating good structural validity.

(4) Common Method Bias Test

This study used Harman' s single-factor test to examine common method bias. All items were subjected to unrotated exploratory factor analysis. If more than one factor solution emerged and the largest factor' s explanatory rate was below 40%, common method bias would be considered non-serious. The analysis yielded five solutions, with the largest factor explaining 27.6%, passing the common method bias test.

4.3 Hypothesis Testing

(1) Main Effects Test

Main effects test results are shown in Table 8 . Controlling for gender, age, education level, and quantified self device usage frequency, both perceived severity (β = -0.134, p < 0.05, Model 2) and perceived susceptibility (β = -0.169, p < 0.01, Model 3) significantly negatively affected privacy disclosure intention.

Privacy concern also significantly negatively affected privacy disclosure intention (β = -0.147, p < 0.05, Model 4). Perceived severity (β = 0.265, p < 0.001, Model 8) and perceived susceptibility (β = 0.539, p < 0.001, Model 9) both significantly positively affected privacy concern. Therefore, H1, H2, H3, H4a, and H5a are supported.

(2) Mediation Effect Test

Mediation effect test results are shown in Table 8. Perceived severity' s negative effect on privacy disclosure intention was significant (β = -0.134, p < 0.05, Model 2), and its positive effect on privacy concern was significant (β = 0.265, p < 0.001, Model 8). After adding the mediator privacy concern, perceived severity' s negative effect on privacy disclosure intention became non-significant, but privacy concern' s negative effect on privacy disclosure intention remained significant (β = -0.119, p < 0.05, Model 5), indicating that privacy concern fully mediates the relationship between perceived severity and privacy disclosure intention, supporting H4b.

Perceived susceptibility' s negative effect on privacy disclosure intention was significant (β = -0.169, p < 0.01, Model 3), and its positive effect on privacy concern was significant (β = 0.539, p < 0.001, Model 9). After adding the mediator privacy concern, both perceived susceptibility and privacy concern' s effects on privacy disclosure intention became non-significant (Model 6), indicating that privacy concern does not mediate the relationship between perceived susceptibility and privacy disclosure intention, thus H5b, H6c, and H7c are not supported.

(3) Moderation and Moderated Mediation Effects Test

Moderation test results are shown in Table 9 . Compared with Model 10, Model 11 added the interaction term between privacy concern and technological affordance, which had a significant positive effect on privacy disclosure intention (β = 0.147, p < 0.01), indicating that technological affordance moderates the relationship between privacy concern and privacy disclosure intention, supporting H6a. Similarly, Model 13 shows that boundary management also moderates this relationship (β = 0.177, p < 0.05), supporting H7a.

The moderation effect diagrams are shown in Figure 2 [Figure 2: see original paper]. Compared with lower technological affordance levels, when technological affordance is high, the negative effect of privacy concern on privacy disclosure intention weakens, even showing a positive effect. Similarly, compared with lower boundary management levels, when boundary management is high, the negative effect of privacy concern on privacy disclosure intention weakens, also showing a positive effect. In other words, both technological affordance and boundary management weaken or even reverse the negative effect of privacy concern on privacy disclosure intention. This finding indicates that the privacy paradox phenomenon indeed exists in the quantified self context and reveals its formation mechanism.

Additionally, the joint effect of the two moderators is shown in Table 9. Building

on Model 14, Model 15 simultaneously added the interaction between privacy concern and technological affordance ($\beta = 0.198$, $p < 0.001$) and between privacy concern and boundary management ($\beta = 0.214$, $p < 0.001$), finding that the moderating effects remained significant with increased path coefficients and stronger significance. This indicates that technological affordance and boundary management not only individually weaken the negative effect of privacy concern on privacy disclosure intention but also have a stronger weakening effect when acting together.

This study further explored the effects under different combinations of technological affordance and boundary management levels, with results shown in Table 10 . As technological affordance and boundary management levels increase, the moderating effect gradually changes from negative to positive. Although not all combinations are significant, the overall trend shows that when both are at high levels, their combined weakening effect is strongest (Effect = 0.161, 95% CI = [0.064, 0.259]).

Moderated mediation test results are shown in Table 11 . When technological affordance is low, the mediating effect of privacy concern in the perceived severity → privacy concern → privacy disclosure intention chain is -0.058 (95% CI = [-0.116, -0.019]). At medium technological affordance, the mediating effect is -0.020 (95% CI = [-0.050, 0.007]). At high technological affordance, the mediating effect is 0.017 (95% CI = [-0.012, 0.058]). The moderated mediation effect is significant across three technological affordance levels (Effect = 0.065, 95% CI = [0.025, 0.131]). Therefore, technological affordance moderates the mediating effect of privacy concern between perceived severity and privacy disclosure intention; higher technological affordance weakens the negative mediation, with the effect direction shifting from negative to positive. Similarly, boundary management also significantly moderates this mediating effect (Effect = 0.027, 95% CI = [0.008, 0.056]); higher boundary management weakens the negative mediation, with the effect direction also shifting from negative to positive. Thus, H6b and H7b are supported.

When both moderators were included in the model simultaneously, the moderated mediation analysis is shown in Table 12 . Both technological affordance (Effect = 0.087, 95% CI = [0.038, 0.161]) and boundary management (Effect = 0.034, 95% CI = [0.014, 0.062]) weaken the negative mediating effect of privacy concern between perceived severity and privacy disclosure intention, with effect sizes increasing compared to single moderator effects. This study also further explored how different level combinations of technological affordance and boundary management moderate the mediating effect of privacy concern, as shown in Table 12. As technological affordance and boundary management levels increase from low to high, the moderated mediation effect gradually changes from negative to positive. Although not every level combination is significant, when both are at high levels, the weakening effect is strongest (Effect = 0.066, 95% CI = [0.022, 0.134]).

4.4 Quantitative Research Results

Quantitative research found that in the quantified self context, users' perceived severity and perceived susceptibility not only reduce privacy disclosure intention but also enhance privacy concern, while privacy concern also reduces privacy disclosure intention and mediates the relationship between perceived severity and privacy disclosure intention. Additionally, both technological affordance and boundary management play weakening roles in the relationship between privacy concern and privacy disclosure intention, even reversing the original negative relationship. Simultaneously, they also weaken the negative mediating effect of privacy concern between perceived severity and privacy disclosure intention.

Overall, these results collectively reveal the formation mechanism of the privacy paradox: users' subjective assessment of privacy threats is the key source triggering privacy concern and reducing privacy disclosure intention, and privacy concern further reduces privacy disclosure intention. On this foundation, technological affordance and boundary management prompt users to conduct dynamic trade-offs under concerned conditions, thereby adjusting privacy disclosure intention and presenting the privacy paradox phenomenon.

5 Integration of Qualitative and Quantitative Research

First, qualitative research extracted six main categories through grounded theory three-level coding: privacy concern, privacy disclosure intention, perceived severity, perceived susceptibility, technological affordance, and boundary management, providing a foundation for subsequent model construction. Taking boundary management as an example, qualitative research extracted four subcategories—subjective initiative, boundary rules, boundary management, and boundary coordination—through inductive analysis of interview texts, further aggregating them into the main category of boundary management, reflecting users' active control ability in the privacy disclosure process. In quantitative research, this was measured through items such as "I will selectively provide personal information to this device or application" and "I will set others' access permissions to my information on this device or application," effectively confirming consistency in variable measurement and conceptual categories.

Second, quantitative research showed that privacy concern negatively affects privacy disclosure intention, a conclusion explained in qualitative research. For example, interviewee M7 stated, "I worry my boss will judge workload based on step count, so I choose to turn off this function." Qualitative research also revealed two key triggers for privacy concern and privacy disclosure intention formation—perceived severity and perceived susceptibility. For instance, N9 mentioned, "Now privacy leakage causes society-wide distress, so I worry about privacy issues." N7 mentioned, "This platform has a good reputation; I' ve never seen negative reports about privacy leakage, so my privacy risk concern is weak," both explaining the quantitatively confirmed positive effect of perceived severity and perceived susceptibility on privacy concern. Additionally, some interviewees

believed "I feel disclosing information won' t greatly affect me" (N2) and "I feel the likelihood of this threat happening to me is small, so I confidently disclose privacy" (N3), further explaining the quantitatively confirmed negative effects of perceived severity and perceived susceptibility on privacy disclosure intention.

Third, quantitative research confirmed that technological affordance and boundary management moderate the relationship between privacy concern and privacy disclosure intention. Qualitative interview results showed that even when users have privacy concerns, they may still be willing to disclose privacy information, especially when disclosure can achieve user goals and when users have controllable scope over disclosed privacy. For example, M6 stated, "Although I may worry about data leakage, the convenience and personalized services of health management make me willing to sacrifice some privacy." N8 mentioned, "I will judge the degree myself; if it exceeds my bottom line, I definitely won' t use it." These views further support quantitative research findings.

Finally, this study hypothesized in quantitative research that privacy concern mediates between perceived severity/perceived susceptibility and privacy disclosure intention, and that technological affordance and boundary management moderate privacy concern' s mediating effect. However, empirical results only confirmed that privacy concern mediates between perceived severity and privacy disclosure intention, and that technological affordance and boundary management moderate this mediating effect. Combined with interview content such as "I think the possibility of privacy leakage is high, so I will minimize privacy information permissions" (N10), this study believes that compared to perception of privacy threat severity, users' perception of the likelihood of occurrence may directly inhibit their disclosure intention.

6 Discussion

This study adopted a mixed-methods approach combining qualitative and quantitative research to explore the privacy paradox formation mechanism in the quantified self context. The study found that users' subjective perceptions of privacy threat severity and likelihood trigger privacy concern and reduce privacy disclosure intention, while privacy concern itself also reduces privacy disclosure intention, constituting the basic path of the privacy paradox. Further, under the moderating effects of technological affordance and boundary management, this relationship is reconstructed, enabling users to potentially have high privacy disclosure intention even under high privacy concern, forming the privacy paradox. Specific findings are as follows.

(1) Both perceived severity and perceived susceptibility positively affect privacy concern and negatively affect privacy disclosure intention. Privacy concern negatively affects privacy disclosure intention and mediates the relationship between perceived severity and privacy disclosure intention. This indicates that users' perceived severity and likelihood of privacy threats trigger low privacy disclosure intention and high privacy concern

[54]. Meanwhile, privacy concern further reduces privacy disclosure intention [49]. Additionally, perceived severity can reduce privacy disclosure intention by triggering users' privacy concern.

(2) Technological affordance moderates the relationship between privacy concern and privacy disclosure intention. When technological affordance is high, the negative effect of privacy concern on privacy disclosure intention weakens and may even become positive. Specifically, although users with privacy concern are unwilling to disclose privacy information, to achieve quantified self goals and obtain needed services, they will choose to ignore privacy threats and cede privacy information to service providers in exchange for required services. When users find that technological affordance can indeed achieve goals, their privacy disclosure intention will further strengthen [4]. This not only confirms the existence of the privacy paradox in the quantified self context but also reveals its formation mechanism: under conditions where privacy concern weakens users' privacy disclosure intention, users still tend to disclose privacy to achieve specific goals.

(3) Boundary management also moderates the relationship between privacy concern and privacy disclosure intention. The higher the boundary management level, the weaker the negative effect of privacy concern on privacy disclosure intention, and direction reversal may even occur. Specifically, boundary management endows users with greater initiative and control in privacy management. By managing privacy boundaries, users can effectively control the flow of privacy information between themselves and others and the accompanying privacy risks. Even with privacy concern, users may choose to disclose privacy information because of boundary management, consistent with communication privacy management theory [48]. This reveals another important mechanism of privacy paradox formation: when privacy concern weakens privacy disclosure intention, users' privacy disclosure intention significantly increases when they have strong autonomous control over privacy boundaries.

(4) Both technological affordance and boundary management weaken the negative mediating effect of privacy concern between perceived severity and privacy disclosure intention; the higher their levels, the stronger the weakening effect, consistent with their moderating roles between privacy concern and privacy disclosure intention. Specifically, under high technological affordance, although severe consequences of privacy threats cause user privacy concern, users may still choose to disclose privacy to achieve specific quantified self goals. Under high boundary management, even when users perceive the severity of privacy threat consequences and develop privacy concern, they may believe their control over privacy boundaries can reduce risks and thus be willing to disclose privacy.

7.1 Theoretical Contributions and Managerial Implications

This study makes several theoretical contributions: (1) It examines the privacy paradox phenomenon in the quantified self context, not only expanding research on the privacy paradox in new contexts but also enriching privacy issue research in the quantified self context. (2) It reveals the formation mechanism of the privacy paradox for quantified self users and verifies the boundary conditions for privacy paradox existence. Existing research indicates that privacy paradox existence depends on specific boundary conditions [12], and this study further verifies and expands this view. (3) It incorporates technological affordance and boundary management into the same research framework, explaining user privacy decision-making processes from dual perspectives of technical interaction possibilities and individual privacy control capabilities, revealing their mechanisms in the relationship between privacy concern and privacy disclosure intention, and providing new perspectives for deeply understanding the privacy paradox phenomenon.

Based on the revealed formation mechanism of the quantified self privacy paradox, this study provides managerial implications for relevant government departments and quantified self device/application service providers from three aspects: reducing perceived severity and susceptibility, enhancing privacy management, and improving technological affordance.

(1) Reduce users' perceptions of potential privacy threat severity and susceptibility. Perceived severity and susceptibility are root causes of user privacy concern and reduced privacy disclosure intention, so addressing both can weaken privacy concern and enhance privacy disclosure intention. Relevant government departments should strengthen publicity of privacy protection policies to ensure users fully understand privacy policy protections; analyze typical privacy leakage cases to improve users' rationality regarding privacy risks; increase crackdowns on illegal behaviors such as excessive personal information collection and unauthorized data use; regularly review and assess service providers' data security conditions to create a secure environment for health information services.

(2) Enhance users' privacy literacy and privacy management capabilities. Boundary management is an important reason users are willing to disclose privacy. Relevant government departments and service providers should collaboratively promote user privacy literacy improvement, jointly conduct privacy protection publicity and training to help users master basic privacy management skills; cultivate users' ability to actively manage privacy, encourage them to clarify their privacy boundaries, and promote active disclosure outside boundary ranges; establish user privacy management support platforms to provide privacy issue consultation, help users understand privacy policies, and respond to privacy challenges.

(3) Optimize product design to enhance user privacy management levels and product technological affordance. Technological affordance is another im-

portant reason users are willing to disclose privacy. Therefore, product design should maximize technological affordance while ensuring user privacy security. On one hand, service providers can formulate clear and understandable rights and responsibilities statements through simplified content, highlighted key points, and visualization, allowing users to fully understand the purposes and risks of disclosed information while improving privacy setting flexibility and transparency. On the other hand, innovate and optimize service functions to increase possibilities for meeting users' diverse needs, provide richer user experiences, and promote users' continuous use.

7.2 Limitations and Future Directions

This study has several limitations: (1) It is based on narrow quantified self, focusing on the health domain. Future research can expand to broad quantified self to build more universally applicable theoretical frameworks. (2) The empirical part collected self-reported cross-sectional data. Future research can use multi-time-point sampling methods to enhance conclusion robustness. (3) The research subjects mainly concentrate on young and middle-aged groups with relatively high education levels. Future research can focus on segmented groups such as the elderly and users with different education levels to further verify conclusion universality.

[1] Zhang Q, Xie W H. Privacy disclosure behavior of quantified self: connotative features, theoretical framework and research prospects[J]. Journal of intelligence, 2022, 41(9): 112-120.
[2] Yang M Q, Zhu Q H, Zhao Y X, et al. Quantified self: research development, elements and opportunities[J]. Journal of the China Society for Scientific and Technical Information, 2022, 41(3): 244-253.
[3] Zhang Q, Xie W H, Wang Y J, et al. The influence of antecedent configurations of privacy concerns in quantified self on willingness to disclose privacy: power-responsibility equilibrium perspective[J]. Journal of intelligence, 2024, 43(9): 139-147.
[4] Zhang Q, Xie W H, Wang Z. Research on privacy paradox in quantified self from the perspective of coping theory[J]. Journal of intelligence, 2023, 42(5): 175-183,199.
[5] Oetzel G, Gonja. Online privacy paradox: social representations perspective[C]//Proceedings of the CHI' 11 extended abstracts on human factors in computing systems. Vancouver: ACM, 2011: 2107-2112.
[6] Zhang Y D, Zhang H L, Zhang C B, et al. The driving factors composition of users' privacy concern and the formation mechanism of privacy paradox in social network services[J]. Chinese journal of management, 2022, 19(7): 1046-1055.
[7] Wu D J, Zhu H. The formation mechanism of consumer privacy paradox in online shopping under dual attitude[J]. Journal of intelligence, 2020, 39(8): 160-165,173.

[8] Xiang M M, Sun W T, Feng L. A review on privacy paradox across the world[J]. Library and information service, 2023, 67(4): 134-148.
[9] Geng S P. A qualitative study of young user' s privacy concerns and interactive practice[J]. Journalism & communication review, 2024, 77(3): 15-29.
[10] Bandara R, Fernando M, Akter S. Explicating the privacy paradox: a qualitative inquiry of online shopping consumers[J]. Journal of retailing and consumer services, 2020, 52: 101947.
[11] Dienlin T, Trepte S. Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors[J]. European journal of social psychology, 2015, 45(3): 285-297.
[12] Han X, Tan J. Does the privacy paradox exist? A meta-analysis of the relationship between privacy concerns and privacy behavior[J]. Journal of information resources management, 2022, 12(2): 101-111.
[13] Xu J P, Zhang X Y, Hu T. Beyond quantitative and qualitative researches: the types and application of researches by mixed methods[J]. Journal of Soochow University (educational science edition), 2019, 7(1): 50-59.
[14] Lee V R. What's happening in the "Quantified Self"movement?[C]//Proceedings of the international conference of the learning sciences (ICLS 2014). Boulder: ISLS, 2014.
[15] Maltseva K, Lutz C. A quantum of self: a study of self-quantification and self-disclosure[J]. Computers in human behavior, 2018, 81: 102-114.
[16] Neff G, Nafus D. Self-tracking[M]. Cambridge: The MIT Press, 2016.
[17] Feng S, Xiong H X, Huang J Z, et al. Research on affordances of quantified self technology from the perspective of the grounded theory[J]. Library and information service, 2024, 68(3): 59-70.
[18] Lupton D. The quantified self[M]. Cambridge: Polity Press, 2016.
[19] Hu D H, Zhang Y F. Research on quantified self[J]. Library tribune, 2018, 38(2): 1-7.
[20] Zhang Y, Li J X, Huang B B, et al. Conflict and turbulence of privacy boundaries: a study on the formation mechanism of the privacy paradox in the quantified-self scenario[J]. Information studies: theory & application, 2025, 48(1): 93-103.
[21] Barnes S B. A privacy paradox: social networking in the United States[J]. First monday, 2006, 11(9): 5-16.
[22] Fox G. "To protect my health or to protect my health privacy?" A mixed-methods investigation of the privacy paradox[J]. Journal of the Association for Information Science and Technology, 2020, 71(9): 1015-1029.
[23] Kang H, Jung E H. The smart wearables-privacy paradox: a cluster analysis of smartwatch users[J]. Behaviour & information technology, 2021, 40(16): 1755-1768.
[24] Zhu H, Wang K, Yan Z J, et al. An analysis of privacy paradox phenomenon in SNS users based on privacy calculus[J]. Journal of intelligence, 2017, 36(2): 134-139,121.
[25] Xie X Z, Cai N Z, Huang Z M, et al. Investigation of determinants of social media user privacy paradoxical behavior[J]. Library and information service,

2018, 62(18): 55-63.
[26] Zhu H, Fang Q Y. Quantifying and examining privacy paradox of social media users[J]. Data analysis and knowledge discovery, 2021, 5(7): 111-125.
[27] Xu X T, Zhu Q H. Research on user characteristics and participation patterns in the initial stage of quantified self in perspective of personal health management[J]. Library & information, 2022(5): 51-62.
[28] Strauss A. Qualitative analysis for social scientists[M]. Cambridge: Cambridge University Press, 1987.
[29] Liu X, Xie L S. Joy or concern? The dual-path influence mechanism of service robots' roles on employee wellbeing: a qualitative and quantitative study based on human-robot interaction in the service and hospitality context[J]. Nankai business review, 2025, 28(3): 124-135,160.
[30] Li C N, Bi X H, Chen X Y, et al. Structural dimension and scale development of user engagement with smart wearable health technologies[J]. Chinese journal of management, 2023, 20(6): 887-895.
[31] Mousavi R, Chen R, Kim D J, et al. Effectiveness of privacy assurance mechanisms in users' privacy protection on social networking sites from the perspective of protection motivation theory[J]. Decision support systems, 2020, 135: 113323.
[32] Wu K W, Huang S Y, Yen D C, et al. The effect of online privacy policy on consumer privacy concern and trust[J]. Computers in human behavior, 2012, 28(3): 889-897.
[33] Xue K, He J, Yu M Y. Research on the influencing factors of the privacy paradox in social media[J]. Contemporary communication, 2016(1): 34-38.
[34] Dinev T, Hart P. An extended privacy calculus model for e-commerce transactions[J]. Information systems research, 2006, 17(1): 61-80.
[35] Rogers R W. A protection motivation theory of fear appeals and attitude change1[J]. The journal of psychology, 1975, 91(1): 93-114.
[36] Liu B L, Lei X F, Xu Y. Emotion and context' s impact on users' engagement in defensive privacy protection behaviors[J]. Data analysis and knowledge discovery, 2024, 8(3): 63-76.
[37] Ma X. IS professionals' information security behaviors in Chinese IT organizations for information security protection[J]. Information processing & management, 2022, 59(1).
[38] He X, Liu Y, Li M X. Harnessing the power of online privacy management: exploring affordance considerations[C]//International conference on information systems (ICIS). Bangkok: AIS.
[39] Lu M M, Zhang Y Q. Between the visible and the invisible: research on the self-management practice of the privacy boundary of digital reading traces[J]. Publishing journal, 2025, 33(1): 66-75.
[40] Gibson J J. The ecological approach to visual perception: classic edition[M]. New York: Psychology Press, 2014.
[41] Xie W H, Zeng S M, Peng T P, et al. Technology affordance: conceptual connotation, theoretical framework and prospect[J]. Science and technology management research, 2022, 42(5): 210-218.
[42] Gaver W W. Technology affordances[C]//Proceedings of the SIGCHI

conference on human factors in computing systems. New York: ACM, 1991: 79-84.
[43] Bygstad B, Munkvold B E, Volkoff O. Identifying generative mechanisms through affordances: a framework for critical realist data analysis[J]. Journal of information technology, 2016, 31(1): 83-96.
[44] Naik P, Schroeder A, Kapoor K K, et al. Behind the scenes of digital servitization: actualizing IoT-enabled affordances[J]. Industrial marketing management, 2020, 89: 232-244.
[45] Petronio S. Boundaries of privacy: dialectics of disclosure[M]. New York: State University of New York Press, 2002.
[46] Abdelhamid M. Fitness tracker information and privacy management: empirical study[J]. Journal of medical internet research, 2021, 23(11): e23059.
[47] Zimmer M, Kumar P, Vitak J, et al. There' s nothing really they can do with this information: unpacking how users manage privacy boundaries for personal fitness information[J]. Information, communication & society, 2020, 23(7): 1020-1037.
[48] Gao L, Yuan Q J. Communication privacy management theory and its application and prospect in the field of information system research[J]. Journal of modern information, 2023, 43(5): 168-177.
[49] Wang L Y, Li Q, Qiao Z L, et al. Impact of protection motivation on privacy concerns and privacy security protection behaviors of SNS users[J]. Journal of intelligence, 2019, 38(10): 104-110.
[50] Mohamed N, Ahmad I H. Information privacy concerns, antecedents and privacy measure use in social networking sites: evidence from Malaysia[J]. Computers in human behavior, 2012, 28(6).
[51] Dong X Y, Wang T N. Technical feature, social tie structure and social commerce purchase behavior[J]. Journal of management sciences in China, 2020, 23(10): 94-115.
[52] Xu H, Dinev T, Smith H J, et al. Examining the formation of individual' s privacy concerns: toward an integrative view[C]//Proceedings of the twenty ninth international conference on information systems (ICIS). Paris: AIS, 2008: 1-16.
[53] Cheng X, Hou T, Mou J. Investigating perceived risks and benefits of information privacy disclosure in IT-enabled ride-sharing[J]. Information & management, 2021, 58(6): 103450.
[54] Zang G Q, Guo R Y, Han M. Research on the mechanism of privacy lie flat on privacy protection behavior[J]. Library and information service, 2023, 67(8): 129-140.

(Corresponding author: Yao Shanji E-mail: yaoshanji@126.com)

Author Contributions:
Yao Shanji: Topic selection and design, paper writing and revision;
Liu Wenli: Paper writing and revision;
Liu Jiajing: Research idea discussion, paper revision.

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