Scientific and Social Research, 2024, Volume 6, Issue 3
https://ojs.bbwpublisher.com/index.php/SSR

# The Influence of Self-Efficacy of College Students in Privacy Protection and Behavior in Social Networking Context

**Mingwu Cui[1], Fangfang Ding[1]*, Kun Cai[2]**

[1]School of Journalism and Communication, Anhui University, Hefei 230601, China
[2]School of Big Data and Statistics, Anhui University, Hefei 230601, China

***Corresponding author:*** Fangfang Ding, dff971017@126.com



**Abstract:** In the era of mobile social media, users who show themselves on social platforms will face the risk of privacy breaches. Frequent data leaks and increasingly complex social media privacy protection terms intensify users' privacy concerns, along with mandatory privacy exposure, contributing to privacy fatigue among users. This study examines the changes in privacy protection behavior among college students under the influences of privacy concerns and privacy fatigue from the perspective of self-efficacy in privacy protection. Data is collected through a questionnaire survey, and a structural equation model is established to provide insights into protecting user privacy. The results of this research indicate that college students' internal self-efficacy in privacy protection has a negative impact on privacy fatigue. College students' privacy concerns are significantly negatively correlated with their willingness to disclose information, while privacy fatigue is significantly positively correlated with their willingness to disclose information. Privacy fatigue among college students has a significant positive influence on both their disclosure intention and the behavior of disengaging from privacy protection.

**Keywords:** Privacy protection self-efficacy; Privacy protection behavior; Social network

**Online publication:** March 29, 2024

## 1. Introduction

### 1.1. Research background

In October 2021, the Cyberspace Administration of China released the draft of the Administration of Account Name Information of Internet Users for public comment [1]. Article 12 stipulates that the IP address geographic information of Internet user accounts should be displayed on the account information page. By the end of April 2022, the Chinese social networking platform Weibo fully displayed IP location in comments, showing the provinces for domestic users and countries for foreign users [2]. Subsequently, platforms such as TikTok, Xiaohongshu, and WeChat Official Accounts also implemented this feature. In June 2022, the Cyberspace Administration of China reviewed and approved the Administration of Account Name Information of Internet

Users, amending Article 12 as follows, Internet information service providers should display the geographical information of the Internet protocol (IP) address of Internet user accounts within a reasonable range on the internet user account information page, facilitating public supervision for the public interest. Although the mandatory display of users' IP location does not fall under sensitive data exposure, it still raises public concerns about privacy breaches.

When users show themselves on social networking platforms, they do indeed face the risk of privacy breaches. When going online, users' personal information, browsing history, and more are transformed into data stored on servers. On the surface, users have the freedom to publish and delete content and personal information, as well as erase their online traces. However, numerous cases have confirmed that both the deleted content and the records of their clicks and browsing leave indelible traces on the internet. If online platforms fail to comply with relevant regulations, users are essentially exposed "naked." Recently since May 2021, the National Internet Information Office has reported 351 cases of illegal and irregular collection and use of personal information by mobile applications (apps), and popular apps are not exempt from this data breach [3]. Similar situations can be observed in other countries as well. In April 2021, Facebook was faced with a data leak scandal, where the personal data of over 500 million users, including phone numbers and email addresses, was compromised. In June 2020, Google faced a lawsuit and was accused of privacy breaches involving millions of users, leading to a claim of $500,000.

Frequent private data breaches have intensified users' concerns about privacy protection. The increasingly complex privacy protection terms and mandatory privacy exposure have resulted in privacy fatigue among users. The research conducted by Saadia et al. revealed that only 5% of the surveyed participants would read the legal agreements of mobile applications [4]. According to a survey by Kaspersky Lab, 32% of internet users do not know how to fully protect their privacy online, and 36% of users felt stressed about enhancing privacy protection, indicating a gradual emergence of user privacy fatigue [5]. Under the influences of privacy concerns and privacy fatigue, it is questioned that if users can protect their personal privacy based on their own capabilities, and to what extent will users' willingness to disclose information and their behavior of disengaging from privacy protection be affected.

Existing research on user privacy behavior divides the willingness to disclose personal information into two aspects, disclosure intention and disengagement behavior. Regarding users' disclosure intention, Degirmenci proposed that users' previous privacy experiences, perceived control, and concerns about app permissions have varying degrees of influence on users' privacy concerns, thereby affecting their intention to use apps [6]. Wang et al. analyzed the willingness of app users to disclose personal information from the perspectives of perceived benefits and perceived risks [7]. In terms of disengagement behavior, Xu et al. explored the influence of self-efficacy in privacy protection on the intention of social networking users to disengage, with privacy fatigue acting as a mediating variable [8]. Choi et al. incorporated both users' disclosure intention and disengagement behavior into their research model, proposing that privacy fatigue and privacy concerns have varying degrees of influence on them [9].

This study selects college students as the research subjects because they are an active online population and are expected to have a strong awareness of privacy protection. The research analyzes users' self-efficacy in privacy protection from both internal and external dimensions. It also introduces the variables of privacy concerns and privacy fatigue. The goal is to explore the relationship between college students' self-efficacy in privacy protection and their willingness to disclose personal information and engage in disengagement behavior in the context of social networking. The aim is to provide insights into user privacy protection behavior.

### 1.2. Research objectives

The research objectives of this article are as follows.

First, to construct a research model on the influence of college students' privacy protection self-efficacy on their privacy protection behavior.

Secondly, Collecting data through questionnaire surveys, utilizing AMOS 24.0 to fit structural equation models, exploring the influence of internal and external privacy protection self-efficacy of social networking users on privacy concerns and privacy fatigue, as well as whether users' privacy concerns and privacy fatigue will negatively affect their privacy protection behavior, namely, positively influencing users' willingness to disclose information and their engagement in privacy disengagement.

Thirdly, to contribute to the theoretical research on privacy fatigue theory through specific case analysis, and to inspire better protection of the privacy of social networking users in practice.

### 1.3. Research content

The paper is divided into six sections, with the specific research content as follows.

Section 1: Introduction. In this chapter, the research background, objectives, and content are discussed.

Section 2: Theoretical foundation. This chapter elaborates on the concepts of privacy protection self-efficacy, privacy concerns, privacy fatigue, willingness to disclose personal information, and privacy disengagement behavior, laying the theoretical foundation for the subsequent research.

Section 3: Research model and hypotheses. This chapter proposes a model of factors influencing college students' privacy protection behavior in the context of social networking through literature analysis.

Section 4: Research methods and data analysis. This chapter clarifies the research methods used in the paper, which are literature analysis, questionnaire surveys, and structural equation modeling. It describes how the questionnaire was designed, data collected, and empirical analysis conducted to validate the model and hypotheses.

Section 5: Findings and implications. This chapter summarizes the research findings and implications, which include theoretical implications and practical implications.

Section 6: Research limitations and future directions. This chapter highlights the limitations of the study and provides suggestions for future research directions.

## 2. Theoretical foundation

Privacy research involves disciplines such as law, communication, psychology, sociology, and computer science. This article draws on the definition of privacy in the civil code and defines data privacy as the private space, activities, and information of a natural person that is recorded in the form of personal data or depicted in digital form which is not intended to be known by others [10].

### 2.1. Privacy protection self-efficacy

Bandura defines self-efficacy as the belief in one's capabilities to organize and execute the courses of action required to produce given goals [11]. In this study, privacy protection self-efficacy refers to the user's confidence in their ability to protect their personal data privacy from the impact of data collection and sharing activities when using social networking platforms.

Based on attribution theory research, Xu et al. divided privacy protection self-efficacy into two dimensions, internal and external [8]. Internal privacy protection self-efficacy represents an individual's belief in their own abilities, that is, their perceived capability to independently protect their personal privacy. Just like a user

familiar with appliances who believe they don't need to read the instruction manual, some social networking users, based on their previous privacy protection experiences, believe they can protect their own privacy information. When internal privacy protection self-efficacy is high, individuals rely less on external support to learn or guide their privacy protection behaviors. External privacy protection self-efficacy represents an individual's belief in protecting their privacy information, but this belief is not based on their own experiences or abilities but rather comes from external sources such as the assistance of others. Therefore, external privacy protection self-efficacy refers to individuals' perception of their ability to protect their privacy with the support of at least one other individual.

## 2.2. Privacy concerns

Privacy concerns, also known as privacy worries or privacy anxieties, are defined by Hong et al. as the perceived risk or worry regarding the potential loss of control over personal information or exposure to undesired consequences as a result of information disclosure or privacy-invasive practices [12]. It reflects the degree of concern that internet users have regarding the potential disclosure of their personal information in the online space and represents a subjective perception and attitude. Research showed that 80% of smartphone users have concerns about their personal data online [13]. In this study, considering the characteristics of social networks and the personal information of social network users, privacy concerns are defined as users' perceptions and concerns regarding the collection, acquisition, monitoring, and use of their personal information. In terms of privacy attitudes, which refer to users' attitudes toward privacy issues, privacy concerns are considered a central concept for measuring privacy attitudes in the field of information management [14]. In the context of social interactions, privacy concerns are widely applied in research on privacy issues and user behavior. Nearly all empirical studies on privacy attitudes and privacy behaviors have utilized the concept of privacy concerns [15].

## 2.3. Privacy fatigue

The concept of fatigue refers to an unpleasant emotional state in the medical field [16]. When individuals are required to handle more tasks in the decision-making process than they can effectively manage, they often experience this fatigue [17]. Fatigue arises from situations where individuals facing excessive demands are unable to achieve their goals, and the primary manifestation of fatigue is the inability to make decisions. Previous research on fatigue has also indicated that it can lead to a lack of coping ability and avoidance behaviors.

Privacy fatigue reflects a sense of weariness among internet users regarding privacy issues. This fatigue arises from the complexity of online privacy protection and an underestimation of the risks of data breaches, leading to a decrease in users' attention to privacy concerns [18]. Individuals who experience privacy fatigue tend to reduce their decision-making efforts regarding privacy protection [19]. On the internet, privacy protection agreements or policies are becoming increasingly complex and opaque, requiring users to invest significant effort in managing their online personal information. This often results in users giving up on reading and understanding privacy protection agreements and simply checking "I accept", especially when they need to click on a link to view the full text [20].

Hargittai et al. introduced the concept of online apathy to address the issue of a lack of privacy protection behavior among American Internet users [21]. Zang et al. constructed a mechanism model for privacy helplessness based on the theory of learned helplessness, using Sina Weibo as an example [22].

The survey and analysis conducted by Choi et al. on 324 internet users revealed that privacy fatigue has a greater impact on privacy behavior than privacy concerns, despite the latter being widely regarded as the

primary factor explaining online privacy behavior [9].

### 2.4. Intention to disclose personal information

Privacy disclosure generally refers to the self-disclosure of personal information. Self-disclosure is a prerequisite for self-expression and communication with others, involving five dimensions, which are intention, breadth, depth, accuracy, and nature. Intention refers to the voluntary nature of self-disclosure, breadth refers to the duration and frequency of disclosure, depth refers to the intimacy of disclosure, accuracy refers to the truthfulness of the disclosed information, and nature refers to positive or negative disclosure [23]. Previous studies have shown that internet activities require a significant amount of personal information disclosure. Online self-disclosure reduces uncertainty in interactions, legitimizes one's identity in online groups, and is also necessary when purchasing goods or services where users need to disclose their real personal information [24].

Currently, research on privacy disclosure by social media users mainly focuses on perspectives such as privacy calculus theory and planned behavior theory. Based on the assumption of users as rational beings, it suggests that privacy disclosure on social media is a rational behavior made after weighing the pros and cons. When users perceive that the benefits outweigh the risks, they choose to disclose their privacy. The privacy disclosure decisions of social media users are not entirely rational processes. According to a meta-analysis conducted by Li et al., habitual behavior has a greater impact on privacy disclosure intentions compared to perceived risks and benefits [25]. This indicates that users' disclosure of personal information on social platforms may be more of an unconscious habit.

In addition, Puneet et al. have found in their research on young social media users that there is a positive correlation between the subjective well-being and self-disclosure inclination of young users on the internet [26].

### 2.5. Privacy protection disengagement behavior

Privacy protection detachment stems from the concept of detachment. Detachment is defined as efforts to reduce processing pressure or even attempts to escape from the interference of pressure [27]. It manifests as disengagement from the intended task rather than seeking solutions to the problem. When faced with privacy threats, social network users may enhance their management of personal information protectively, including restricting the scope of information disclosure, posting false information, and carefully examining privacy policies provided by websites. However, the increasing difficulty of privacy protection and the growing frequency of data breaches may make individuals feel unable to control their personal information, ultimately leading to the abandonment of their privacy protection behavior, resulting in privacy protection detachment [28]. The phenomenon of privacy protection detachment indicates that social network users give up various coping behaviors when facing privacy threats.

## 3. Research models and hypotheses

### 3.1. Internal privacy protection self-efficacy, concerns, and fatigue

Privacy self-efficacy refers to the perception and belief of users in their ability to control personal information and space when it comes to protection. Xing et al. pointed out that individuals who are confident in their privacy information management abilities can reduce privacy concerns [29]. In other words, users with lower self-efficacy are more concerned about their privacy because they feel incapable of deciding when and how to provide access to their personal information.

Choi et al. conducted a study and found that as users' self-efficacy increases, they tend to consider their personal behavior more deeply [30]. For example, they assess whether their actions could result in privacy

breaches, which channels could potentially lead to leaks, and what measures to take in the event of a breach. Under these circumstances, users with high internal self-efficacy have greater confidence in their ability to protect their privacy, which may lead to lower levels of privacy concerns.

In the study conducted by Johansson et al. on patients, it was found that self-efficacy can alleviate negative emotions in cancer patients, such as fatigue [31]. In the research conducted by Xu et al. on the privacy behaviors of social network users, it was found that internal privacy self-efficacy has a negative impact on privacy fatigue [8].

Therefore, this paper proposes the following assumptions:

H1(a): Internal privacy protection self-efficacy of college students has a negative impact on privacy concerns.

H1(b): Internal privacy protection self-efficacy of college students has a negative impact on privacy fatigue.

## 3.2. External privacy protection self-efficacy, concerns, and fatigue

External privacy self-efficacy reflects the belief of users in their ability to utilize external assistance. In terms of privacy protection, compared to users with high internal privacy self-efficacy, users with high external self-efficacy have minimal privacy protection experience and may even feel incapable. They hold a pessimistic attitude towards their own privacy protection abilities and express concerns about privacy breaches.

Morrisonew's study shows that reliance on others often incurs a social cost [32]. Therefore, for users with high external privacy self-efficacy, the increase in social costs also intensifies their sense of fatigue. In Xu et al.'s research on the privacy protection behaviors of social network users, it is revealed that high external privacy self-efficacy exacerbates the level of privacy fatigue experienced by social network users [8].

Based on this, this paper proposes the following assumptions:

H2(a): College students' external privacy protection self-efficacy has a positive impact on privacy anxiety.

H2(b): College students' external privacy protection self-efficacy has a positive effect on privacy fatigue.

## 3.3. Privacy concerns and privacy fatigue

The study conducted by Bright et al. indicates that social media users who are highly concerned about privacy are more likely to experience stress and fatigue [33]. In Ren's research on the factors influencing negative usage behavior on social media in China, it is pointed out that privacy concerns have a positive impact on users' social media fatigue [34]. Amandeep et al. explored the impact of social media fatigue on users and highlighted that users' privacy concerns have a positive influence on social networking service fatigue [35].

Based on the above research, this paper proposes the following hypotheses:

H3: College students' privacy concerns have a positive impact on privacy fatigue

## 3.4. Privacy concerns, intention to disclose personal information, and privacy protection disengagement behavior

Several studies have confirmed that users' willingness to disclose their privacy is directly influenced by the level of privacy concerns. Phelps et al. found that privacy concerns have a negative impact on self-disclosure [36]. Aldhafferi et al. found that university students with stronger privacy concerns tend to limit the visibility of their content, reduce self-disclosure, and are less willing to expand their social networks to avoid privacy risks [37]. The meta-analysis by Yu et al. verified the negative impact of perceived privacy risk and privacy concerns on the willingness to disclose privacy and also discovered the moderating effect of platform type [38]. In comparison to emotional platforms, the influence of perceived privacy risk and privacy concerns on disclosure willingness is stronger in functional platforms. In social networking contexts, users tend to reduce their willingness to

disclose privacy due to concerns about the collection or secondary use of their personal data.

Excuse behavior refers to an individual's effort to reduce the effort required to deal with stressors or even give up attempts to intervene in stressors to achieve goals [39]. The study by Son and Kim shows that individuals with high privacy concerns tend to have lower excuse behavior [40]. Jia et al.'s research on the factors influencing personal information security and privacy protection behaviors of social network users demonstrates that users with higher privacy concerns are more capable of perceiving privacy risks [41]. As a result, they consciously adopt proactive security measures to prevent their personal information security and privacy from being compromised.

Therefore, this paper proposes the following assumptions:

H4(a): College students' privacy concerns have a negative impact on their willingness to disclose personal information

H4(b): College students' privacy concerns have a negative impact on disengagement from privacy protection

## 3.5. Privacy fatigue, intention to disclose personal information, and privacy protection disengagement behavior

Privacy fatigue reflects a sense of weariness among internet users regarding privacy issues. This fatigue arises from the complexity of online privacy protection and an underestimation of privacy breach risks, leading to a decreased level of user attention towards privacy concerns. Choi et al. found that privacy fatigue positively impacts individuals' willingness to disclose personal information [9].

Wang et al. discovered that negative privacy fatigue emotions result in users' reduced motivation and initiative in addressing privacy issues, leading to various degrees of privacy fatigue behavior such as tolerance, neglect, and withdrawal [42]. Xu et al. found a significant positive correlation between privacy fatigue and the detachment from privacy protection among social network users [8].

Therefore, this paper proposes the following assumptions:

H5(a): College students' privacy fatigue has a positive impact on their willingness to disclose personal information

H5(b): College students' privacy fatigue has a positive effect on privacy protection disengagement

## 3.6. Research model

Based on the assumptions proposed above, a research model is established, as shown in **Figure 1**.

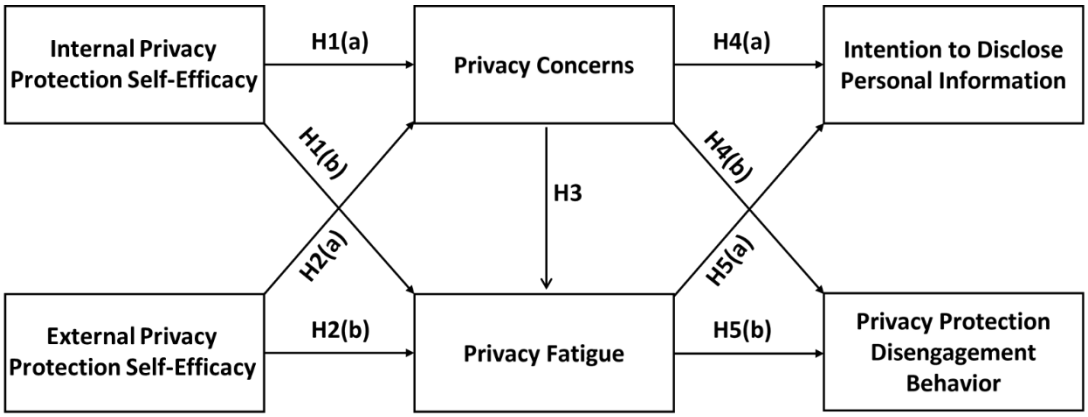


**Figure 1**. Relationship between research models and assumptions

# 4. Research methods and data analysis

## 4.1. Research methods

### 4.1.1. Literature analysis method

The literature analysis method refers to the approach of collecting and organizing literature to form a scientific understanding of facts. In this paper, through keyword searches on academic websites such as CNKI, Web of Science, and Elsevier, relevant literature and research findings were systematically collected and organized to grasp the research progress in this field and clarify the theoretical basis and practical significance of the research. Through the analysis of the literature, potential influencing factors of social networking users' privacy protection behavior were identified and summarized, laying the theoretical foundation for the entire study.

### 4.1.2. Questionnaire survey method

The questionnaire survey method is a survey method that uses uniformly designed questionnaires to understand the situation and solicit the opinions of respondents. Its key steps include setting questionnaire subjects, selecting survey subjects, and analyzing the results data. The data in this paper are derived from survey questionnaires. This study adapted existing mature scales and made appropriate modifications based on practical application scenarios. Questionnaires were distributed to college students to understand the influencing factors of their privacy protection behavior in the context of social networking.

### 4.1.3. Structural equation modeling

Structural equation modeling (SEM) belongs to the empirical analysis method, which is a research method that uses examples and experiences to infer and illustrate theories. This includes steps such as determining the topic, proposing hypotheses, collecting data, testing and analyzing, and drawing conclusions. In this paper, SEM is utilized to conduct an empirical analysis of questionnaire data. Specifically, SPSS Statistics 25 is mainly used for reliability and validity analysis of the sample data, while AMOS 24 is employed to analyze and demonstrate the influencing factor model of online users' privacy protection behavior, verifying the rationality of the model and hypotheses.

Researchers like Fotis investigated 266 social media users and conducted data analysis using SEM to investigate the determinants that affect users' trust in shared information related to travel acquired from social media or tourism sites to provide valuable insight into travelers' behavior and managerial implications of sharing information from social network sites [43].

## 4.2. Sample data collection

This study primarily utilized a questionnaire survey for data collection, targeting college students as the population of interest among social network users. The questionnaire was distributed online, and the survey period was from May 19, 2022, to May 25, 2022. A total of 330 questionnaires were distributed and collected. The collected questionnaires were rigorously screened and exempted according to the following criteria.

Respondents who had not used any social network platforms, data showing a high level of similarity (over 80%), and response time below 120 seconds. After the screening process, 277 valid questionnaires were obtained, resulting in a response rate of 83.9%.

## 4.3. Questionnaire settings

The survey questionnaire consists of two sections, which are respondent information and measurement variables. The measurement variables were selected from well-established and widely cited scales as shown in **Table 1**, considering the psychological characteristics of domestic users. The measurement variables were

assessed using a 5-point Likert scale with 1 representing strongly disagree and 5 representing strongly agree.

**Table 1.** Questionnaire measurement variables and sources

| Latent variable | Test variable | Source |
|---|---|---|
| Internal privacy self-efficacy (PSEI) | I can protect my privacy without guidance<br>I can protect my privacy if the social networking platform provides instructions for use<br>I can protect my privacy without having any experience with similar social networking platforms | Thatcher et al. [44] |
| External privacy protection self-efficacy (PSEE) | I can protect my privacy if someone helps me<br>I can protect my privacy if someone guides me<br>I can protect my privacy if someone can give me a demonstration<br>I can protect my privacy if the social networking platform I use is reliable | Thatcher et al. [44] |
| Privacy concerns (PC) | I am concerned that the information submitted to the service provider of the social networking platform may be misused by the platform<br>I am concerned that someone will find my private information on social networking platforms<br>I am concerned about providing personal information to social networking platforms, as it may be used by others | Liao et al. [45] |
| Privacy fatigue (PF) | I am tired of social network privacy concerns<br>I am not so keen on protecting the personal information I provide to social networking platforms<br>I am starting to doubt the importance of online privacy concerns | Choi et al. [46] |
| Intention to disclose personal information (IDPI) | I am willing to provide personal information when using the social networking platform in the future<br>I may disclose my personal information on social networking platforms if necessary<br>I may authorize the personal information which social networking platform asks for | Choi et al. [46] |
| Privacy protection disengagement behavior (PPDB) | If the personal information provided to the social network is misused, I would take the following actions:<br>I will not think about dealing with the problem<br>I will give up the idea of solving this problem<br>I will give up the act of solving this problem | |

## 4.4. Data Analysis

### 4.4.1. Data Analysis Methods

This study primarily used SPSS 23.0 and AMOS 24.0 for data organization and statistical analysis. SPSS 23.0 was primarily used for the pre-processing of big data, descriptive data analysis, and reliability and validity data analysis. AMOS 24.0 was primarily used for conducting structural equation modeling analysis.

### 4.4.2. Descriptive statistics

The characteristics of the survey sample in this study are shown in **Table 2**. 83.75% of the respondents reported daily social network usage exceeding 4 hours, indicating that the majority of the sample was moderate to heavy users of social networking platforms, which is beneficial for studying their privacy behaviors on social networking platforms.

**Table 2.** Sample descriptive statistics

| Category | Variable | Number of people | Percentage (%) |
|---|---|---|---|
| Gender | Male | 102 | 36.82% |
| | Female | 175 | 63.18% |

**Table 2 (Continue)**

| Category | Variable | Number of people | Percentage (%) |
|---|---|---|---|
| Highest education level (including current study) | College | 4 | 1.44% |
| | Undergraduate | 157 | 56.68% |
| | Graduate and above | 116 | 41.88% |
| Time spent on social networks | 1–3 hours | 45 | 16.25% |
| | 4–6 hours | 124 | 44.77% |
| | 7–9 hours | 80 | 28.88% |
| | More than 9 hours | 28 | 10.11% |
| Specialization | Science | 30 | 10.83% |
| | Engineering | 41 | 14.80% |
| | Medicine | 4 | 1.44% |
| | Agronomy | 3 | 1.08% |
| | Literature | 130 | 46.93% |
| | History | 12 | 4.33% |
| | Philosophy | 2 | 0.72% |
| | Economics | 12 | 4.33% |
| | Management | 21 | 7.58% |
| | Law | 9 | 3.25% |
| | Pedagogy | 4 | 1.44% |
| | Art | 9 | 3.25% |

### 4.4.3. Reliability and validity testing

First, the reliability and validity of the questionnaire were evaluated. In this study, composite reliability (CR) was used to assess the reliability of the questionnaire, and average variance extracted (AVE) and Cronbach's alpha coefficient were used to assess the validity of the scale variables in the questionnaire as shown in **Table 3**.

**Table 3.** Factor loading, Cronbach's alpha coefficient, CR, AVE of measurement indicators

| Variable | Factor | Factor Loadings | CR | AVE | Cronbach's Alpha |
|---|---|---|---|---|---|
| Internal self-efficacy (PSEI) | PSEI1 | 0.832 | 0.859 | 0.671 | 0.858 |
| | PSEI2 | 0.843 | | | |
| | PSEI3 | 0.780 | | | |
| External self-efficacy (PSEE) | PSEE1 | 0.896 | 0.853 | 0.609 | 0.840 |
| | PSEE2 | 0.904 | | | |
| | PSEE3 | 0.809 | | | |
| | PSEE4 | 0.402 | | | |
| Privacy concerns (PC) | PC1 | 0.765 | 0.863 | 0.680 | 0.853 |
| | PC2 | 0.746 | | | |
| | PC3 | 0.948 | | | |

**Table 3 (Continue)**

| Variable | Factor | Factor Loadings | CR | AVE | Cronbach's Alpha |
|---|---|---|---|---|---|
| Privacy fatigue (PF) | PF1 | 0.668 | 0.799 | 0.572 | 0.794 |
| | PF2 | 0.844 | | | |
| | PF3 | 0.747 | | | |
| Intention to disclose personal information (IDPI) | IDPI1 | 0.517 | 0.773 | 0.542 | 0.755 |
| | IDPI2 | 0.810 | | | |
| | IDPI3 | 0.839 | | | |
| Privacy Protection Disengagement Act (PPDB) | PPDB1 | 0.813 | 0.874 | 0.699 | 0.869 |
| | PPDB2 | 0.931 | | | |
| | PPDB3 | 0.755 | | | |

For the reliability analysis, the CR values of each latent variable are all greater than 0.7, indicating that the factors have good indicator reliability. The Cronbach's alpha coefficients are all greater than 0.7, indicating that the scale variables of the questionnaire have good internal consistency. The AVE values are all greater than 0.5, indicating that the scale variables of the questionnaire have good convergent validity.

For the validity analysis, the square root of the VAE values of each factor was compared with the inter-variable correlation coefficients to examine the discriminant validity of the scale, as shown in **Table 4**.

**Table 4.** Validity analysis of validation factors

| Variable | PSEI | PSEE | PC | PF | IDPI | PPDB |
|---|---|---|---|---|---|---|
| PSEI | 0.817 | | | | | |
| PSEE | 0.386 | 0.795 | | | | |
| PC | 0.126 | 0.337 | 0.817 | | | |
| PF | -0.162 | -0.022 | -0.011 | 0.762 | | |
| IDPI | 0.050 | -0.007 | -0.188 | 0.107 | 0.732 | |
| PPDB | -0.192 | -0.114 | -0.162 | 0.416 | 0.292 | 0.830 |

From **Table 4**, it can be observed that the square root of each variable (values on the diagonal) is greater than the correlation coefficients between variables (values in the columns below the diagonal). This indicates that the model has good discriminant validity.

### 4.4.4. Model fitting

This study primarily utilized the structural equation model (SEM) method to test the proposed equation. The structural equation model is a statistical analysis method that examines the relationships between variables by analyzing their covariance. It has wide applications in the field of social science. SEM is also a mainstream quantitative research method in domestic research focusing on privacy issues.

Before conducting the structural equation model analysis, this study first examined the measurement model to ensure its good fit and then proceeded with a comprehensive evaluation of the structural equation model. The goodness-of-fit of the structural equation model was measured using indices such as $\chi^2$/df (chi-square divided by degrees of freedom), goodness-of-fit index (GFI), adjusted goodness-of-fit index (AGFI), and root mean

square error of approximation (RMSEA). The data obtained from the questionnaire were imported into AMOS 24.0 software for fitting analysis, and the results are presented in **Table 5**. Based on previous research, it is generally considered that GFI and AGFI values should be greater than 0.9, RMSEA value should be less than 0.08, and $\chi^2$/df should be less than 3. According to the observed results, the fitting indices obtained from this questionnaire met the above criteria, indicating a good level of fit for this model.

**Table 5.** Validation factor analysis table

| Common indicators | Chi-squared degrees of freedom ratio $\chi^2$/ df | GFI | RMSEA | IFI | CFI | TLI | NNFI |
|---|---|---|---|---|---|---|---|
| Judgment standard | <3 | >0.9 | <0.10 | >0.9 | >0.9 | >0.9 | >0.9 |
| Confirmatory factor analysis model | 2.105 | 0.904 | 0.063 | 0.943 | 0.942 | 0.927 | 0.927 |
| Structural Equation Modeling | 2.215 | 0.896 | 0.066 | 0.935 | 0.934 | 0.920 | 0.920 |

### 4.4.5. Hypothesis testing

The hypothesis testing results of this study are presented in **Table 6**. Except for hypotheses H1(a), H2(b), H3, and H4(b), all other hypotheses received varying degrees of support. External privacy protection self-efficacy had a significant positive impact on privacy concerns, privacy concerns had a significant negative impact on privacy disclosure intention, and privacy fatigue had a significant positive impact on both disclosure intention and privacy disengagement behavior.

**Table 6.** Test results of hypotheses

| Assumption | Path | Normalized path coefficients | Conclusion |
|---|---|---|---|
| H1(a) | PSEI-PC | 0.038 | Not Support |
| H1(b) | PSEI-PF | -0.207 ** | Support |
| H2(a) | PSEE-PC | 0.254 *** | Support |
| H2(b) | PSEE-PF | 0.014 | Not Support |
| H3 | PC-PF | 0.019 | Not Support |
| H4(a) | PC-IDPI | -0.203 *** | Support |
| H4(b) | PC-PPDB | -0.164 | Not Support |
| H5(a) | PF-IDPI | 0.215 *** | Support |
| H5(b) | PF-PPDB | 0.520 *** | Support |

Note: *, **, and ***, indicate 10%, 5%, and 1% significance levels, respectively.

# 5. Findings and implications

## 5.1. Research findings

### 5.1.1. Privacy fatigue and self-efficacy

The results of this study indicate that college students' internal privacy protection self-efficacy has a negative impact on privacy fatigue, which is consistent with the relationship between self-efficacy and fatigue in other studies. Anderson et al.'s research confirms that self-efficacy not only predicts protective behavior but also moderates individuals' responses to specific threats [47]. In other words, self-efficacy can effectively reduce negative emotions such as fatigue. However, this study failed to confirm a significant impact between external privacy protection self-efficacy and privacy fatigue, which is inconsistent with the findings of Xu et al. [5].

Possible explanations are that students can conveniently access and grasp privacy protection-related knowledge from various sources with the development of mobile internet and the improvement of digital literacy, thereby avoiding the fatigue associated with frequent external support seeking. Another explanation Xu et al. pointed out is the instability of self-efficacy, which can be influenced by momentary emotions, leading to measurement errors in self-reported self-efficacy results [5].

### 5.1.2. Privacy concerns and self-efficacy

This study failed to confirm a significant impact between privacy protection self-efficacy and privacy concerns, which is inconsistent with the findings of Yu et al. [48]. However, Youn similarly found that internet privacy protection self-efficacy had no significant impact on privacy concerns [49]. One possible explanation is that college student users are overly confident in their own ability to protect their privacy, to the extent that they never worry about the negative consequences of privacy breaches happening to them. This is related to the psychological phenomenon known as optimistic bias, where individuals tend to overestimate their own abilities and believe that positive events are more likely to occur to them, while negative events are more likely to happen to others.

### 5.1.3. Privacy concerns, privacy fatigue, and willingness to disclose privacy

This study revealed a significant negative correlation between college students' privacy concerns and privacy disclosure intention, as well as a significant positive correlation between privacy fatigue and privacy disclosure intention. Fotis et al. have also confirmed that users are highly concerned about the prospect of their personal information being collected on the Internet without their knowledge by the developer of a social media platform or by online businesses. As users' perceptions of the value of their social media accounts decline, they are more likely to deactivate their accounts to protest how their personal data is improperly processed by the social media platform's developer or online corporations [43]. This indicates that, on one hand, college students control information disclosure due to concerns about the misuse of their personal data, such as setting a three-day visibility limit for their social media posts or making their posts visible only to followers. On the other hand, due to frequent privacy breaches and the desire for more convenient services, social network users experience privacy fatigue, leading them to inappropriately disclose personal information to platforms.

This indicates that on one hand, college students control information disclosure due to concerns about personal data misuse, such as setting social media accounts to be visible only to followers, or hiding real information when posting. On the other hand, due to factors such as frequent privacy breaches and high sunk costs, college students experience privacy fatigue, causing them to improperly disclose personal information to platforms [50].

### 5.1.4. Privacy concerns, fatigue, and protection disengagement

Disengagement from engagement is one of the key outcomes of fatigue [52]. This study once again confirmed this conclusion in the context of data privacy protection behavior among college students. The research results of this article showed that privacy fatigue among college students had a significant positive impact on their disclosure intention and privacy disengagement behavior. The long-term benefits of data privacy protection did not motivate users who were already fatigued with privacy protection. There are two possible reasons for this phenomenon: first, users underestimate the risks of privacy breaches; second, frequent privacy breaches or even forced exposure of privacy lead users to believe that their concerns or measures taken for privacy protection are futile.

This study shows that user concerns about privacy breaches do not have a negative impact on privacy

disengagement. This suggests that although repeated data breaches increase people's concerns about privacy, individuals ultimately engage in privacy disengagement behavior due to their doubts about their ability to make effective decisions and take measures to protect their privacy. This is consistent with the findings of Wang et al. in their survey on privacy concerns among Chinese and American college students [53]. College students disclose personal privacy information online because the expected benefits of online privacy are increasing, and there are more opportunities for disclosure. With the deep integration of the internet into daily life, the immediate benefits of privacy disclosure in terms of convenience, mental enjoyment, and material gains become apparent, while privacy risks are perceived as probabilities of loss, making it difficult to have a direct deterrent effect. It becomes challenging to accurately assess the trade-off between benefits and risks. This also demonstrates the limitations of privacy calculus theory in the digital age.

Furthermore, this study indirectly verifies the findings of Choi et al., which states that although privacy concerns are considered a primary factor in explaining online privacy behavior, privacy fatigue has a greater impact on privacy behavior than privacy concerns [9].

## 5.2. Research implications

### 5.2.1. Theoretical implications

This paper makes two main theoretical contributions. First, it investigates the influencing factors on privacy protection behaviors of college students when using social networks, which are privacy concerns and privacy fatigue. These factors have a negative impact on users' privacy protection behaviors. Secondly, the paper confirms that internal privacy protection self-efficacy is the influencing factor of privacy fatigue.

### 5.2.2. Practical implications

The practical significance of this paper lies in exploring the influencing factors of social media users' privacy protection to inspire better user privacy protection. Measures can be taken from three dimensions, which are technology, platform, and policy, to protect the privacy of social media users.

In terms of technology, the privacy of social media users can be protected through methods such as encrypting data. Some scholars have protected patient privacy by developing EHR systems that encrypt patient data [54].

Regarding platforms, social media platforms can alleviate user privacy fatigue by simplifying privacy protection terms and beautifying interface design to help users understand privacy protection terms and give them more choices. Existing research has confirmed that high-level interface design perception, privacy protection self-efficacy, and privacy knowledge are important factors in alleviating user privacy fatigue [55].

In terms of policy, countries should formulate and adhere to rules to guide technology towards goodness. The results of this study show that frequent data breaches are a major cause of privacy fatigue among college students, and disengagement is a key outcome of this fatigue. Privacy fatigue leads users to engage in privacy disengagement behavior. The fact that personal information has become a legal issue requiring protection is a result of the development of information network technology. To protect personal information, it is necessary to prioritize the role of technology and laws that guide technology toward positive outcomes. Whether the rules are scientifically formulated or not will guide and even determine the behavior of market participants. Strict adherence to rules and regulations can better protect users' privacy. It should not solely rely on the conscience of individual companies but should establish rules to influence technology. If legislation is a long-term solution, mandatory national standards can be developed, but precautions should be taken to prevent these standards from being influenced by internet giants.

## 6. Research limitations and future directions

The biggest limitation of this study is the sample issue. First is the sampling method. Using online questionnaires inherently limits the range of respondents, resulting in a concentration of respondents from colleges in a specific region. Although internet usage is not directly linked to geographical location, the impact of sample randomness on the results cannot be ignored. Second, the sample consists of college students, who are skilled in internet usage and generally belong to a group with high privacy concerns and anxieties. Therefore, the generalizability of the conclusions is limited. However, the study did not sufficiently consider the trust level of the sample users towards online platforms or their experiences of privacy infringement. With a total of 277 valid questionnaires in this study, the sample size certainly affects the generalizability of the survey results. This study is based on the use of social networking software and examines the relationship between the internal and external efficacy of personal privacy protection, privacy concerns, privacy fatigue, and the resulting changes in privacy behavior. However, it did not adequately consider other influencing factors such as emotions on privacy concerns and privacy fatigue. The current research limitations provide directions for future research efforts. The team will strive to expand the coverage of samples and increase their randomness in the future, considering more influencing factors, to make modest contributions to the privacy protection of social networking users.

## Funding

This paper is supported by the National Social Science Fund of China under grant No.18BXW042.

## Disclosure statement

The author declares no conflict of interest.

## References

[1] The Cyberspace Administration of China, 2021, Notice of the State Internet Information Office on the Public Consultation on the Provisions on the Management of Internet User Account Name Information (Draft for Comments). http://www.cac.gov.cn/2021-10/26/c_1636843202454310.htm

[2] The Cyberspace Administration of China, 2021, Regulations on the Management of Internet User Account Information. http://www.cac.gov.cn/2022-06/26/c_1657868775042841.htm

[3] Jin Y, 2021, Investigation and Analysis Report on Personal Privacy Data Leakage in the Era of Big Data. Journal of Tsinghua University (Philosophy and Social Sciences), 36(1): 191–201 + 206.

[4] Saadia N, Mohamed B, Belaid B, 2023, Privacy Conditions Changes' Effects on Users' Choices and Service Providers' Incomes. International Journal of Information Management Data Insights, 3(1): 100173.

[5] Kaspersky, 2019, The True Value of Digital Privacy: Are Consumers Selling Themselves Short? https://www.kaspersky.com/blog/privacy-report-2019/.

[6] Degirmenci K, 2020, Mobile Users' Information Privacy Concerns and the Role of App Permission Requests. International Journal of Information Management, 2020(50): 261–272.

[7] Wang T, Duong TD, Chen CC, 2016, Intention to Disclose Personal Information via Mobile Applications: A Privacy Calculus Perspective. International Journal of Information Management, 36(4):531–542.

[8] Xu Y, Li H, Yu L, 2019, Research on the Influence of Self-efficacy of Privacy Protection on Privacy Behavior of Social Network Users. Library and Information Service, 63(17): 128–136.

[9] Choi H, Park J, Jung Y, 2018, The Role of Privacy Fatigue in Online Privacy Behavior. Computers in Human

Behavior, 81(4): 42–51.

[10] Sheng X, Jiao F, 2021, Data Privacy Governance from the Perspective of Domestic Laws and Regulations. Library Tribune, 41(6): 85–99.

[11] Bandura A, 1977, Self-efficacy: Toward a Unifying Theory of Behavioral Change. Psychological Review, 84(2): 191–215.

[12] Hong W, Thong JYL, 2013, Internet Privacy Concerns: An Integrated Conceptualization and Four Empirical Studies. MIS Quarterly, 37(1): 275–298.

[13] Kwon J, Johnson ME, 2015, The Market Effect of Healthcare Security: Do Patients Care about Data Breaches? Workshop on the Economics of Information Security. The Netherlands, Delft.

[14] Wang X, Zhao Y, Zhu Q, 2015, Review on User Privacy Concerns in Social Media Context. Journal of the China Society for Scientific and Technical Information, 34(12): 1322–1334.

[15] Zhang X, Li Z, 2018, Information Privacy Concerns, Trust and Information Security Behavior Intention of Smartphone Users. Modern Intelligence 38(3): 45–50.

[16] Piper BF, Lindsey AM, Dodd MJ, 1987, Fatigue Mechanisms in Cancer Patients: Developing Nursing Theory. Oncology Nursing Forum, 14(6): 17.

[17] Acquisti A, Friedman A, Telang R, 2006, Is There a Cost to Privacy Breaches? An Event Study. Twenty-seventh International Conference on Information Systems (ICIS). Milwaukee, USA, 1563–1580.

[18] Jonathan, Levav, Mark, et al., 2010, Order in Product Customization Decisions: Evidence from Field Experiments. Journal of Political Economy, 118(2): 274–299.

[19] Schermer BW, Custers B, Simone VDH, 2014, The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection. Ethics and Information Technology, 16(2): 171–182.

[20] Zhu H, Zhang M, Lu Y, 2018, An Empirical Study on Privacy Policy Reading Intention of Social Media Users. Journal of the China Society for Scientific and Technical Information, 37(4): 362–371.

[21] Hargittai E, Marwick AE, 2016, What Can I Really Do? Explaining Online Apathy and the Privacy Paradox. International Journal of Communication, 2016(10): 3737–3757.

[22] Zang G, Dong WA, 2022, Study on the Formation Mechanism of Privacy Helplessness: Taking the Social Network Sina Weibo as an Example. Information Studies (Theory & Application) 45(9): 110–118.

[23] Wheeless LR, Grotz J, 1976, Conceptualization and Measurement of Reported Self-disclosure. Human Communication Research, 2(4): 338–346.

[24] Taddei S, Contena B, 2013, Privacy, Trust and Control: Which Relationships with Online Self-Disclosure. Computers in Human Behavior, 29(3): 821–826.

[25] Li X, Huang L, Chen J, 2022, Influencing Factors of Social Media Users' Intentions to Disclose Privacy. Data Analysis and Knowledge Discovery, 6(4): 97–107.

[26] Puneet K, Nazrul I, Anushree T, 2021, Social Media Users' Online Subjective Well-Being and Fatigue: A Network Heterogeneity Perspective. Technological Forecasting and Social Change, 2021(172), 121039.

[27] Youn S, 2009, Determinants of Online Privacy Concern and Its Influence on Privacy Protection Behaviors Among Young Adolescents. The Journal of Consumer Affairs, 43(3): 389–418.

[28] Carver CS, Scheier MF, Weintraub JK, 1989, Assessing Coping Strategies: A Theoretically Based Approach. Journal of Personality and Social Psychology, 56(2): 267–283.

[29] Zhang X, Liu S, Chen X, et al., 2018, Health Information Privacy Concerns, Antecedent, and Information Disclosure Intention in Online Health Communities. Information & Management, 55(4): 482–493.

[30] Choi SS, Choi MK, 2007, Consumer's Privacy Concerns and Willingness to Provide Personal Information in Location-Based Services. Advanced Communication Technology, The 9th International Conference on IEEE 2007,

2196–2199.

[31] Johansson AC, Brink E, Cliffordson C, et al., 2018, The Function of Fatigue and Illness Perceptions as Mediators Between Self-efficacy and Health-related Quality of Life During the First Year After Surgery in Persons Treated for Colorectal Cancer. Journal of Clinical Nursing, 27(7): 1537–1548.

[32] Morrison EW, 1993, Newcomer Information Seeking: Exploring Types, Modes, Sources, and Outcomes. Academy of Management Journal, 36(3): 557–589.

[33] Bright LF, Kleiser SB, Grau SL, 2015, Too Much Facebook? An Exploratory Examination of Social Media Fatigue. Computers in Human Behavior, 44(3): 148–155.

[34] Ren S, 2020, An Empirical Study on the Influencing Factors of Social Media Negative Behaviors: Taking WeChat as an Example. Proceedings of the 15th Annual Conference of China Management 2020. Chinese Academy of Management, Chengdu, 1218–1230.

[35] Dhir A, Kaur P, Chen S, et al., 2019, Antecedents and Consequences of Social Media Fatigue. International Journal of Information Management, 2019(48): 193–202.

[36] Phelps J, Nowak G, Ferrell E, 2000, Privacy Concerns and Consumer Willingness to Provide Personal Information Journal of Public Policy & Marketing, 19(1): 27–41.

[37] Aldhafferi N, Watson C, Sajeev A, 2013, Personal Information Privacy Settings of Online Social Networks and their Suitability for Mobile Internet Devices. International Journal of Security Privacy and Trust Management, 2(2): 1–17.

[38] Lu Y, He L, Wu H, et al., 2019, A Meta-Analysis to Explore Privacy Cognition and Information Disclosure of Internet Users. International Journal of Information Management, 51(1): 102015.

[39] Carver CS, Scheier MF, Weintraub JK, 1989, Assessing Coping Strategies: A Theoretically Based Approach. Journal of Personality and Social Psychology, 56(2): 267–283.

[40] Son JY, Kim SS, 2008, Internet Users' Information Privacy-Protective Responses: A Taxonomy and a Nomological Model. MIS Quarterly, 32(3): 503–529.

[41] Jia R, Wang X, Fan X, 2021, Empirical Study on Influencing Factors of SNS Users' Personal Information Security and Privacy Protection Behavior. Journal of Modern Information, 41(09): 105–114 + 143.

[42] Wang M, Hou G, You Z, 2021, Research on Influencing Factors and Behavioral Choice of Internet Users' Privacy Fatigue: Based on S-S-O Theory and Grounded Theory. Information Studies (Theory & Application), 44(09): 149–154 + 128.

[43] Kitsios F, Mitsopoulou E, Moustaka E, et al., 2022, User-Generated Content Behavior and Digital Tourism Services: A SEM-neural Network Model for Information Trust in Social Networking Sites. International Journal of Information Management Data Insights, 2(1): 100056.

[44] Thatcher J, Zimmer J, Gundlach M, et al., 2008, Internal and External Dimensions of Computer Self-Efficacy: An Empirical Examination. Engineering Management, 55(4): 628–644.

[45] Liao CC, Liu CC, Chen KC, 2011, Examining the Impact of Privacy, Trust and Risk Perceptions Beyond Monetary Transactions: An Integrated Model. Electronic Commerce Research and Applications, 10(6): 702–715.

[46] Choi H, Park J, Jung Y, 2018, The Role of Privacy Fatigue in Online Privacy Behavior. Computers in Human Behavior, 2018(81), 42–51.

[47] Anderson CL, Agarwal R, 2010, Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions. Mis Quarterly, 34(3): 613–643.

[48] Yu T, Yang Y, 2019, Privacy Concerns in Online Behavioral Advertising. Journalism Research, 2019(09): 101–116 + 121.

[49] Youn S, 2009, Determinants of Online Privacy Concern and Its Influence on Privacy Protection Behaviors Among Young Adolescents. Journal of Consumer Affairs, 43(3): 389–418.

[50] Zhu M, Wu C, Huang S, et al., 2021, Privacy Paradox in Health Applications: An Integrated Elaboration Likelihood Model Incorporating Privacy Calculus and Privacy Fatigue. Telematics and Informatics, 2021(61): 101601.

[51] Demerouti E, Mostert K, Bakker AB, 2010, Burnout and Work Engagement: A Thorough Investigation of the Independency of Both Constructs. Journal of Occupational Health Psychology, 15(3): 209–222.

[52] Hopstaken JF, Linden DVD, Bakker AB, et al., 2015, A Multifaceted Investigation of the Link between Mental Fatigue and Task Disengagement. Psychophysiology, 52(3): 305–315.

[53] Wang M, Jiang Z, 2017, A Comparative Study on Online Privacy Concerns of Chinese and American College Students Based on Privacy Computing Theory: A Case Study of 462 College Students in H Province of China and State I of the United States. Contemporary Communication, 2017(06): 77–79 + 84.

[54] Redwan W, Karuna P, Seung G, 2024, Leveraging Semantic Context to Establish Access Controls for Secure Cloud-Based Electronic Health Records. International Journal of Information Management Data Insights, 4(1): 100211.

[55] Liu B, Li J, 2023, Study on the Influence Mechanism of Users' Information Privacy Behavior from the Perspective of Both Technical Characteristics and Individual Differences. Journal of Modern Information, 43(04): 137–149 + 164.