RESEARCH ARTICLE

European Journal of Humanities and Social Sciences
www.ej-social.org

Social Media Use and Privacy Concerns: How do College Students view Internet Privacy and Information Protection?

Huan Liu and Yanling Wang

ABSTRACT

The study is to prove the intermediary effect of privacy concerns, explore the attitude toward online privacy on social media, and summarize the privacy protection strategies adopted by college students on China's mainland. We used the questionnaire to collect the data from college students. The questionnaire was conducted online and offline, and students at Hebei University were randomly selected as the questionnaire object (n = 304). The results show: (1)Privacy concerns fail to mediate the effect of perceived risks on information protection. (2)Affected by perceived risks, most students are worried about online privacy. (3)The current situation of college students' privacy protection is not optimistic. Finally, the paper summarised some privacy protection strategies for college students.

Keywords: Hebei University, Information Protection, Privacy Concerns, Privacy Paradox, Social Media.

Published Online: April 10, 2023

ISSN: 2736-5522

DOI: 10.24018/ejsocial.2023.3.2.429

H. Liu
School of Journalism and Communication, Tianjin Normal University, Tianjin, China.
(e-mail: tianshiliuhuan@gmail.com)
Y. Wang *
School of Journalism and Communication, Tianjin Normal University, Tianjin, China.
(e-mail: wangyl9608@126.com)

Corresponding Author

I. Introduction

In the 1990s, Manuel Scott (1997) made numerous forward-looking researches on the network society, using connection instead of communication to study online social communication. In the 2020s, people have entered the era of mobile new media, and mobile social media has become an essential tool for their daily life. According to the latest data, by the end of 2021, the global online population reached 4.9 billion, accounting for approximately 63% of the world population (Wu & Zeng, 2022).We have entered the network society that Manuel Scott said. People rely more on the Internet and mobile intelligent devices to carry out their online survival and life. With the development of network society, network privacy issues have attracted much attention. The significant difference between privacy in the era of big data and traditional privacy lies in the digitalization of privacy. When intelligent devices store our behavior trajectory in the cloud through the network, our information is stored forever in the form of data.

The social platform provides a place for people to show and communicate freely, which causes the public and private spheres have become increasingly blurred. Personal privacy information, which belongs to the private domain, is released and shared by people in the public domain and becomes shared information. “We play many roles and wear many different masks” (Goffman, 1959). The ambiguity of the role always makes us hesitate when we make a speech. Perhaps what we fear is that private information is taken out of context and disclosed to strangers. And these strangers are easy to be misjudged, which leads to the human flesh search engine or cyber-bullying. More seriously, due to the “permanent storage” feature of the information, a person's past mistakes may forever hinder his future opportunities.

Based on the above potential privacy and security risks of social networks, it is necessary to study the cognitive status of social media users regarding online privacy and security, their level of concern about privacy and security, and privacy protection measures that users can take, and summarize the impact factors of variables such as privacy concerns. Considering the actual situation, this article selects young college students as the research object to investigate their relevant privacy cognition and behavior.

II. Literature Review

A. Influencing Factors Leading to the Difference in Privacy Concerns

Though many people are anxious about internet privacy, their degree of privacy concerns is different. Previous studies have shown that Individual differences (age, gender, online experience), nationality, and national culture significantly affect Internet users' concerns about online privacy (Cho, 2009).

Specific influencing factors are as follows:

1) Age: One research on the privacy concerns of different age groups found that the elderly (over 65 years old) were more worried about the threat to their privacy caused by other people's behavior (Kerzner, 2016). Amandeep (2017) also found that young people had more privacy problems than teenagers and adults, and women were more concerned about privacy than men.
2) Past experiences: College students' past negative experiences of online privacy exposure significantly increased their concerns and perceived risks of online privacy (Yang, 2014).
3) Belief: Religious beliefs affect materialism, which reduces privacy concerns (Alhouti *et al*., 2016). Yao (2008) also found that privacy belief was the most important predictor of their concerns about online privacy.
4) Contact frequency: Xu (2018) found a significant positive correlation between users' media contact frequency on traditional and social media and their privacy concerns.
5) Interpersonal relationship: Hong (2017) found that parents' interpersonal trust and privacy concerns could affect adolescent privacy' concerns (Hong, 2017).
6) The government and platform: Anic (2016) found the weakness of government regulation had deepened users' concerns about their privacy and security, while the government's online regulatory capacity regulation was seen as weak. Also, lacking corporate privacy responsibility and regulatory protection deprived consumers of privacy authorization, which aroused privacy concerns(Bandara, 2020).

Unlike these researches, this current study focuses on the psychological process of personal privacy concerns. Then we will discuss the causes of privacy concerns in detail.

B. Concerns about Privacy may not Trigger Protective Actions

Generally, individuals will reduce or even refuse personal disclosure and adopt protective measures because of concerns about privacy leaks (Zhou, 2020). But in 2006, Barnes found in a survey on the network usage of Facebook student users that they paid more attention to privacy but failed to take enough protective actions. Brown (2007) put forward the privacy paradox to explain and solve the inconsistency between privacy attitude and privacy behavior. He insisted that although people were concerned about their privacy security, they were willing to provide detailed information to online retailers if there was a corresponding return. Norberg (2007) formally established the concept of privacy paradox and defined it as people cannot predict their network behavior according to their views on network privacy. Tufekcida (2008)also found that online privacy concerns had little impact on information disclosure. Thus, although users are worried about the risks of information disclosure, they also choose to actively share personal privacy by weighing the expected benefits of sharing information (Lee, 2013). Finally, Zhang's (2020) empirical study on college students in Nanjing, China, confirmed the existence of the privacy paradox in the social media field. Hence, this study deems that the privacy paradox exists in college students' use of social media.

C. The Information Protection Behavior

Past studies by Cho (2009) found that people had three potential dimensions of privacy protection behavior — avoidance, opt-out and active protection. These dimensions can still explain personal information protection behavior. In addition, these protective measures are closely related to media literacy. Privacy literacy, belonging to media privacy, performs a vital role in enhancing the use of privacy safeguards (Baruh, 2017). Under the guidance of media literacy, people can take active measures when facing privacy threats. For example, the students can address unnecessary concerns by tweaking the visibility of their profiles and using nicknames (Tufekci, 2008). On the Facebook platform, untagging or removing a tag on a shared photo was the most popular and acceptable strategy for managing online privacy (Dhir *et al.*, 2016). These specific strategies are conceived and implemented with the support of media literacy.

Considering the limitation of this questionnaire in our survey, we are hard to predict whether college students will take protective measures into practice under privacy threats. To supplement the explanation of the action part of the theoretical framework, we assume that the positive attitude towards information protection indicates that they will take protective measures. Hence, the evaluation of these information protection behaviors"(question 7 in the questionnaire) is equal to the information protection(IP) part of this theoretical framework. But this assumption is contrary to the privacy paradox. To support this hypothesis and eliminate the privacy paradox, we discuss the causes and corresponding strategies of the privacy paradox.

D. The Pivacy Calculus Theory

Wolfe and Laufer (1999) introduced the social exchange theory in economics into user research and called the procession of user analysis and evaluation Privacy Calculus. The Privacy Calculus holds that users decide whether to upload personal information based on the assessments of benefits and risks. Relevant empirical research supports the Privacy Calculus theory (Milne & Rohm, 2000).

As the issue of online privacy becomes more important, the Privacy Calculus theory is crucial in explaining the behavior of users' online privacy disclosure. To polish the theory, we make some adjustments. Firstly, the traditional theory ignores the consideration of people's emotional or attitudinal factors. Hence, we add a new influencing factor, namely privacy concerns, which may play a significant role in taking protection measures. In addition, we take information protection behavior as the research core instead of privacy disclosure. This change can enrich the dimension of privacy behavior.

III. Research Hypothesis

A. Questions and Hypotheses

Next, considering the existing literature, we bring two specific research questions and five research hypotheses.

a) RQ1: Do privacy concerns play a mediating role in the information processing path of "perceived risks- privacy concerns- information protection"?
b) RQ2: What is the attitude of college students towards privacy protection regarding social media? What are the crucial influencing factors?

The definition of perceived risks refers to the possible loss caused by the abuse or illegal use of a user's personal information, which is the user's expectation of the worst result (Wu, 2019). Individuals will express concerns about private security in psychology if they perceive that their privacy may suffer losses. Previous studies found that perceived risks usually positively affect privacy concerns. For example, Chellappa and Sin (2005) confirmed the positive correlation between perceived risks and privacy concerns. Thus, there is a positive correlation between privacy risks and privacy concerns (Dinev *et al*., 2011). In addition, users will take protective measures to protect their privacy when they perceive privacy threats, such as reducing privacy disclosure. Moon (2000) also believes that perceived risks will affect users' bodies and emotions and indirectly reduces people's privacy disclosure to protect their information security. It is assumed that:

H1a: Perceived risks have a positive impact on privacy concerns.

H2a: Perceived risks have a positive impact on information protection behavior.

Privacy protection is a self-protection measure adopted by people when they feel the risk of privacy disclosure (Turow & Hennessy, 2007). Milne *et al*. (2004) found that private concerns positively affected users' privacy protection behaviors. Feng *et al*. (2014) analyzed teenagers' social network privacy protection behavior and pointed out that teenagers who received privacy attention and intensive education would take more privacy protection behavior. Those college students with intensively strong privacy concerns tend to limit the visibility of their content and reduce self-disclosure to avoid privacy risks. If they feel a latent menace to privacy, they may take further measures to protect themselves (Choi *et al*., 2018). Nam (2006) and Bansal (2010) showed that privacy concerns could significantly affect individual privacy disclosure intention. It is assumed that:

H3a: Privacy concerns positively affect information protection behavior.

Perceived benefits mainly refer to the sense of belonging to the organization and more interpersonal relationships that individuals can get by disclosing privacy (An & Li, 2013). Maslow's Hierarchy of Needs (1943) denotes that people need belonging and love. And people need to establish emotional ties with others and belong to some group. Therefore, the desire for social capital may reduce users' concerns about privacy and open privacy boundaries. In addition, perceived benefits could affect users' attitudes toward information disclosure (Li, 2015). Tien Wang *et al*. (2016) also found that privacy benefits could affect the disclosure intention of Internet users. Privacy disclosure is logically negatively related to privacy protection. That is, privacy disclosure emphasizes opening the privacy boundaries to share personal information in the public domain. But the core logic of privacy protection is to limit the disclosure of personal information on social media. Based on this, we assume that perceived benefits will positively affect privacy disclosure but negatively affect the implementation of information protection. It is assumed that:

H1b: Perceived benefits negatively affect privacy concerns.

H2b: Perceived benefits negatively affect information protection behavior.

B. Model Construction

Based on existing research findings on privacy concerns, this article contextualizes the privacy concerns of college students into the current social network environment. The paper also constructed a theoretical model through the above research assumptions. We expected to test the relationship between privacy concerns and related variables through the following research model.

European Journal of Humanities and Social Sciences
www.ej-social.org

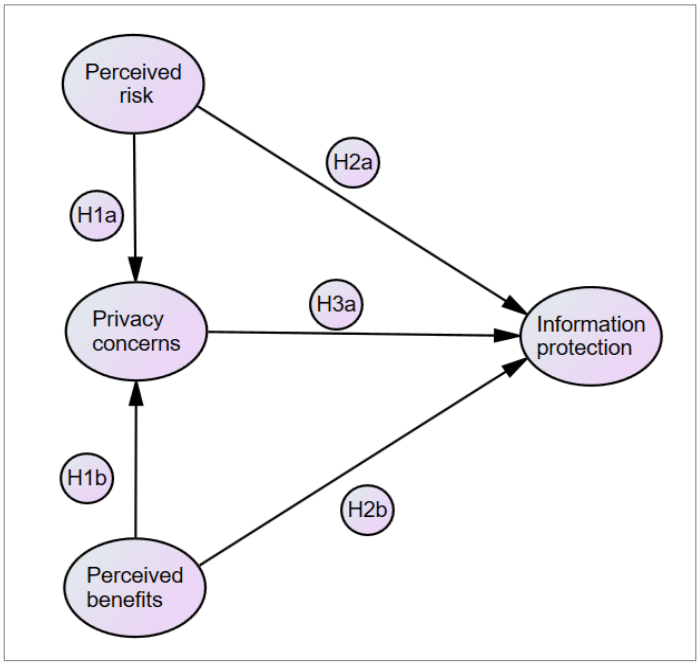

Fig. 1. Theoretical framework.

IV. Research Method

A. Data Sources

The paper questionnaire was randomly distributed and collected on campus, and the electronic questionnaire was put in and collected on the "questionnaire star" platform. The researchers selected Hebei University as the survey site and randomly distributed questionnaires to the students. The author randomly invited students to fill in the paper questionnaire on campus and obtained the electronic questionnaire on WeChat and QQ group chat. The survey time of the questionnaire was from June 10 to June 24, 2021. And we carried out the second batch of questionnaire collection from September 1 to September 10, 2022. The 310 questionnaires and 304 valid samples were collected in this experiment(including 123 electronic and 181 paper questionnaires), and the qualified rate was 98.06%. The data analysis software is SPSS 17.0, and the structural equation modeling software is Amos 25.0.

B. Measurement Index and Source

To test the relationship between variables in the model, the author made appropriate modifications based on relevant research and added new measurement variables, as shown in Table I.

TABLE I: Measurement Index

Perceived risks (PR)	I think it's dangerous to submit personal information to social media. Submitting personal information to social media may lead to privacy leakage. Social media may improperly use submitted personal information. Providing personal information to social media can lead to unexpected problems. I think the information social media asks me is sensitive to me.	Based on Shi Shuo, 2011
Perceived benefits (PB)	Publishing personal information on social media makes me feel like a part of a group. Publishing personal information allows friends on social media to authenticate me. Publishing personal information on social media can make me know more friends.	Based on Shi Shuo, 2011; An Zhaoyu & Liu Luchuan, 2013
Privacy concerns (PC)	How worried are you about social media collecting and analyzing the data you disclose on the Internet? How worried are you that people you don't know will get your information because of your online activities? I'm worried that the information I share on social media may be abused. I'm worried that other people can find personal information about me on social media. I'm worried about providing personal information on social media because others may use it. I'm worried about sharing personal information on social media because it could be used in ways I didn't foresee. I think social media is searching for too much of my personal information. I don't think the way social media stores my personal information is reliable.	Based on Trepte & Masur, 2023; Amandeep, Torbjørn, Ståle & Cecilie S, 2017
Information protection (IP)	Providing false information. Change password regularly. Limit sharing of personal information on social media. Restrict access to personal information. Avoid or restrict the use of online services. Protect the use of social media through technical means.	Based on Quan-Haase & Ho, 2020; Anic, Škare & Milaković, 2019

There are five questions under perceived risks, three questions under perceived benefits, eight questions under privacy concerns, and six questions under information protection behavior. All the items in the scale were composed of "1 = totally disagree" to "5 = totally agree".

C. Reliability And Validity of the Questionnaire

As can be seen from Table II, Cronbach's alpha and Cr are greater than 0.7, the average variance extraction value (AVE) of perceived risks, perceived benefits and privacy concerns is greater than 0.5, and the average variance extraction value of information protection is less than 0.5. In view of this, the author deleted the inappropriate value of standard load and the corresponding items (PR5, PC7, PC8, IP1, IP6), adjusted the model, and obtained the following charts and data.

TABLE II: RELIABILITY AND VALIDITY TEST

Latent variable	Observed variables	Standard load	Cronbach's alpha	CR	AVE
Perceived risks	PR1	0.819	0.864	0.8679	0.5743
	PR2	0.850			
	PR3	0.789			
	PR4	0.771			
	PR5	0.511			
Perceived benefits	PB1	0.802	0.766	0.8562	0.665
	PB2	0.808			
	PB3	0.836			
Privacy concerns	PC1	0.731	0.885	0.9157	0.5763
	PC2	0.757			
	PC3	0.818			
	PC4	0.764			
	PC5	0.759			
	PC6	0.712			
	PC7	0.762			
	PC8	0.766			
Information protection	IP1	0.683	0.714	0.8398	0.4696
	IP2	0.633			
	IP3	0.767			
	IP4	0.744			
	IP5	0.722			
	IP6	0.536			

TABLE III: RELIABILITY AND VALIDITY TEST (REVISED VERSION)

Latent variable	Observed variables	Standard load	Cronbach's alpha	CR	AVE
Perceived risks	PR1	0.813	0.892	0.8917	0.673
	PR2	0.844			
	PR3	0.821			
	PR4	0.803			
Perceived benefits	PB1	0.817	0.766	0.8592	0.6705
	PB2	0.799			
	PB3	0.840			
Privacy concerns	PC1	0.733	0.889	0.8992	0.5981
	PC2	0.743			
	PC3	0.824			
	PC4	0.780			
	PC5	0.781			
	PC6	0.776			
Information protection	IP2	0.651	0.740	0.8283	0.548
	IP3	0.798			
	IP4	0.738			
	IP5	0.766			

We can see from Table III that the Cronbach's alpha coefficients of the four modified variables are more than 0.7, CR is more than 0.7, and the AVE value of convergence validity is more than 0.5. We can see that the combination reliability and convergence validity of the questionnaire are better. Before factor analysis, we performed KMO and Bartlett spherical tests. Results as shown in Table IV, the KMO value is 0.854, and the significance level is 0.000, which indicates that the correlation between cross-sections is significant. And factor analysis can be carried out.

TABLE IV: KMO AND BARTLETT'S TEST

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		0.854
Bartlett's Test of Sphericity	Approx. Chi-Square	2460.477
	df	136
	Sig.	0.000

Table V shows the test results of the discriminant validity. The square root value of the latent variable AVE on the diagonal is greater than the pairwise correlation coefficient between the latent variables, indicating that the scale has good discriminant validity.

TABLE V: DISCRIMINANT VALIDITY TEST

	Perceived risks	Perceived benefits	Privacy concerns	Information protection
Perceived risks	0.820	-	-	-
Perceived benefits	0.056	0.819	-	-
Privacy concerns	0.017	0.584	0.773	-
Information protection	-0.032	0.405	0.354	0.740

The analysis shows that the combined reliability, convergent validity, and discriminant validity of the questionnaire meet the requirements. So we can construct a formal model.

D. Constructing Structural Equation Model

We can see from Table VI that the χ2 value of this research model is 246.410, the χ2/df value is 2.181, the GFI value is 0.908, the AGFI value is 0.876, the RMSEA value is 0.062, the NNFI value is 0.902, the CFI value is 0.944, and the IFI value is 0.944. The above test indexes meet the model test statistics, indicating that the model fitting of this research is acceptable.

TABLE VI: DATA FITTING RESULTS OF STRUCTURAL EQUATION MODEL

Data fitting results of structural equation model								
Index	χ^2	χ^2/df	GFI	AGFI	RMSEA	NNFI	CFI	IFI
Research results	246.410	2.181	0.908	0.876	0.062	0.902	0.944	0.944

E. Mediation Model Test

As shown in Table VII, according to the path analysis of perceived benefits on privacy concerns and information protection behavior, the two paths from perceived risks to information protection and perceived benefits to privacy concerns are deleted because the P-value is too large. Therefore, we only need to analyze the mediating role of privacy concerns in the perceived risks of information protection behavior.

TABLE VII: PATH COEFFICIENT AND P VALUE

			Estimate	S.E.	C.R.	P	Label
Privacy concerns	<---	Perceived risks	0.582	0.065	8.972	***	-
Privacy concerns	<---	Perceived benefits	-0.012	0.048	-0.263	0.793	-
Information protection	<---	Privacy concerns	0.121	0.058	2.090	0.037	-
Information protection	<---	Perceived risks	0.207	0.063	3.295	***	-
Information protection	<---	Perceived benefits	-0.029	0.037	-0.770	0.441	-

TABLE VIII: MEDIATING EFFECT OF PRIVACY CONCERNS ON PERCEIVED RISKS AND PRIVACY CONCERNS

	Variable	Direct Effects - Lower Bounds (BC)	Direct Effects - Upper Bounds (BC)
Direct effect	Perceivedrisks → Privacy concerns	0.419	0.739
	Privacyconcerns → Information protection	-0.015	0.269
	Perceived risks. → Information protection	0.088	0.372
		Indirect Effects - Lower Bounds (BC)	Indirect Effects - Upper Bounds (BC)
Indirect effect	Perceived risks → Privacy concerns	0.00	0.00
	Privacy concerns → Information protection	0.00	0.00
	Perceived risks → Information protection	-0.002	0.166

According to Table VIII, in the impact of perceived risks on personal information protection behavior, network privacy concerns contain 0 in the 95% confidence interval of indirect effect, which means that the mediating influence t of privacy concerns is not significant.

V. RESULTS

H1a is supported, which indicates that perceived risks rather than perceived benefits play a significant part in privacy concerns. The surrounding risk factors intensify college students' anxiety about online privacy, in which the government, platforms, and other stakeholders also play a role. H2a is supported, indicating that perceived risks other than perceived benefits play a decisive role in deciding whether to take information protection behavior. But given the existence of the privacy paradox, we should not only improve the ability of risk perception but also avoid the emergence of the privacy paradox. Thus, the causes and solutions are necessary for us to sum up. H3a is successfully proved, indicating that privacy concerns have a significant impact on information protection behavior. In the path of "perceived risks- privacy

concerns - information protection", mediating the influence of privacy concerns on perceived risks and information protection is not significant. Hence, perceived risks directly influence information protection behavior, rather than indirectly affecting information protection through privacy concerns.

None of the assumptions(H1b, H2b) related to perceived benefits are supported, indicating that the desire for social capital did not have a significant impact on privacy concerns and information protection behavior. Remarkably, college students doubt that sharing individual information on social media can bring them social capital. And perceived benefits also fail to alleviate the privacy concerns caused by using social media. Due to the single-use scenario and lack of understanding of media functions, they prefer to use social media as an intermediary tool for chatting and ignore the underlying benefits of social media. Hence, these college students lack enough attention to the benefits of social media.

According to answers to Q7 and Q8 in the questionnaire, most respondents approve of these measures, indicating that they harbor fundamental judgment for privacy protection behavior and may take these measures in some scenarios. From the answers to the subjective item Q8, the students put forward some protection measures. But the answer is not optimistic overall. Firstly, for Q8, more than half of them are invalid. There are two possibilities: No intention to answer or a lack of knowledge of corresponding privacy protection measures in their brain. The second situation is worrying. In addition, owing to lacking content, the suggestions on government are meaningless.

VI. Discussion

A. From Perceived Risks to Privacy Protection: Mediating Effect of Privacy Concerns

The mediation effect of privacy concerns is not significant, namely, privacy concerns fail to interfere with the impact of perceived risks on privacy. It is a creative finding of this study. Most existing studies believe that the exertion of perceived risks is through privacy concerns to achieve the impact on privacy protection. However, this study confirms that individuals will directly take privacy protection, facing the risks followed by privacy disclosure, without experiencing a specific psychological process, such as privacy concerns. Combining the Elaboration Likelihood Model (ELM), we find that users face two information processing methods when dealing with privacy information: the central route and the peripheral route. Referring to the EML theory, individuals with strong motivation and ability will consider all aspects of privacy information, carefully evaluate, and finally decide on the final action of privacy disclosure and information protection. But people with weak motivation and ability may take measures immediately after a simple assessment. For example, when sharing daily chores, they will quickly assess the risk factors (even without this process) and take privacy protection measures immediately. But when users make cautious political statements in the public field, they will scrutinize the content they want to publish, form an attitude towards privacy security, and finally act on privacy protection. Thus, people have two unique action routes when disclosing privacy: a) perceived risks- privacy concerns- privacy protection. b) perceived risks- privacy protection- privacy concerns. Hence, the variable of privacy concerns is not a mediating variable but a dependent variable affected by the independent variable of perceived risks in this study.

B. College Students' Pessimistic Attitude about Online Privacy on Social Media

In traditional society, people communicate face-to-face based on interpersonal relationships and can better control their individual information, so they fail to pay much attention to their private security. But in the era of social media, people adapt and rely on social media. The unlimited connection of weak relationships can let individual information be transmitted anywhere. Human flesh search engines and cyber-bullying are all over the Internet. Most of the vital information of individuals can be crawled by technology, making people transparent. Nowadays, the frequent incidents of privacy violations also deepen the concerns of privacy threats. First, the monopoly of the social platform on information may lead to information asymmetry. To obtain the services, users will hand over some data. Yet the users do not know why the platform collects this data and where to apply this data. These platforms hold more and more gigantic user data, accurately push advertisements to users and even predict their behavior. Also, the defects of the privacy protection system of social platforms have buried great hidden dangers for the users' privacy security. Their privacy security mechanism is not perfect, leading to the leakage of individual data. For example, some groups stole the data of 5 million users from the US Facebook platform to conduct targeted propaganda during the 2016 presidential election (Du, 2018). Finally, due to the rapid development of social media, the relevant laws and regulations fail to follow up in time, which leads to an insufficient crackdown on the illegal behaviors of social platforms. Yuan (2019) once said that the privacy problem was essentially an issue of individual rights. Under the far-reaching influence of China's historical-cultural tradition of focusing on the interests of the whole, individual rights have been marginalized or even ignored to some extent. Similarly, Robin Li once stated that Chinese people are not sensitive to privacy and willing to exchange privacy for convenience.

C. The Privacy Paradox: Reflection and Countermeasures

We need to reflect on this phenomenon so that college students can take information protection measures into practice.First, the lack of media literacy is one of the main reasons for the paradox. Because most college students are unsophisticated and lack sufficient privacy literacy, they do not pay more attention to the risks of privacy disclosure when sharing their personal information. Also, other scholars do find that the perceived benefits will affect people's privacy protection behavior. It reminds us of balancing the relationship between perceived benefits and information disclosure. Due to the inertia of users themselves, they may provide more information so that platforms and algorithms can better understand their needs and provide more accurate content. But providing more personal information to the platform will make individuals transparent people. Besides, the platform ignores individual demand for privacy control, leaving users powerless when facing the widespread dissemination of private information. Because these platforms deprive consumers of privacy authorization, people are hard to take protective measures(Bandara *et al*., 2020). Prior studies by Aguirre (2016) have tended that giving consumers the right to control their privacy can reduce the occurrence of the privacy paradox, which enables users to close the privacy boundary in time when facing privacy threats. Finally, we need to pay attention to China's unique cultural tradition. Compared with the western individual value orientation, China's ethical value orientation focuses more on public values and collective interests, emphasizing the dedication and attachment of personal interests to collective interests (Qin & He, 2011). Therefore, the desire to gain recognition and support from the online community will make individuals release private messages under privacy risks.

D. Privacy Protection Strategies for College Students

Above all, we summarize them into these suggestions from the survey results:

1) Download official social apps from legitimate app stores and avoid ambiguous apps.
2) Understand the privacy policies of social platforms.
3) Avoid or reduce the submission of facial information on the platform.
4) Restrict the access of social platforms to personal information.
5) Avoid providing the real name, address, and contact information.
6) Prohibit strangers from accessing personal information.
7) Turn off the positioning function of the mobile intelligent device.
8) Change passwords regularly, and avoid using consent passwords.
9) Strengthen the awareness of rights protection, and protect their privacy through legal channels.

Besides, college students can carry out symbolic encryption coding of their information, which can only let specific groups know their true meaning, that is, to create a small-scale subculture symbol communication system. Lastly, They ought to control the release of personal information to express our desire to a certain extent. Even on some strongly connected platforms, such as WeChat, the dissemination of personal privacy, especially portrait information, to the "circle of friends" in the open field may still be maliciously created and spread by people around us.

E. Personal Information Protection Still Needs the Support of External Factors

As for social media, consolidating consumer privacy authorization and alleviating privacy contract infringement are two independent mechanisms to solve online privacy issues(Bandara *et al*.,2020). On the one hand, the platforms consolidate self-discipline and prohibit illegal invasion of personal privacy. For example, the platform needs to be authorized by the user and notified in time before accessing personal information. The process of processing data should also be transparent. On the other hand, the platforms intensify the authorization to users, enhancing users' control over their privacy flow by adding some functions. If the platform grants more privacy management rights to netizens, the netizens can better control the flow of individual information. In addition, consolidate the construction of user databases and guard the security of user data by using an advanced firewall, load balancing, and other technologies. For countries, a perfect legal system has deterrent power and helps to reduce the probability of privacy issues. Relevant departments in China have been actively taking action. China formally implemented the Personal Information Protection Law of the People's Republic of China on November 1, 2021. It stipulates that no organization or individual shall infringe upon the personal information rights and interests of natural persons. But the current laws need refinement to make them more feasible in the future.

VII. Conclusion

This study has two highlights. First, we created a new theoretical framework to study privacy behavior based on the Privacy Calculus theory. This new framework focuses on privacy protection behavior rather than privacy disclosure, which is committed to exploring the adoption of information protection and influencing factors when college students share private information. The innovation of the theoretical focus also provides a new perspective for later scholars to study privacy behavior.

Second, under the guidance of the polished theoretical framework, we carried out a questionnaire survey and verified the relationship between perceived risks, perceived benefits, privacy concerns, and information protection behavior using data results. These empirical conclusions can support realistic decisions.

With the development of the network society, privacy issues will be more prominent. Understanding netizens' attitudes toward privacy and mastering protective measures when using social media are conducive to solving various privacy issues and the long-term development of social media. We wish the study could remind individuals and society of the importance of online privacy. Future research needs to pay more attention to promoting individual media literacy.

Finally, we need to consider some limitations in this study. The current framework is rooted in the Use Satisfaction theory, ignoring the constraints of the social conditions and environment of the audience and the influence of other variables. Besides, the deficiency of this research is that we only select 304 students as the research sample from Hebei University, and its representativeness needs a check.

FUNDING

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

References

Anić, I-D., Škare, V., & Ivana, K.M. (2019). The determinants and effects of online privacy concerns in the context of e-commerce. *Electronic Commerce Research and Applications, 36,* 100868-100868.

An, Z.Y., & Liu, L.C. (2013). The relationship between SNS users' perceived risks, perceived benefits and privacy concerns. *Mathematical practice and understanding, 02*, 129-139.

Barnes, S.B. (2006). A privacy paradox: Social networking in the United States. *First Monday, 11*(9).

Büchi, M., Just, N. ,& Latzer, M. (2016). Caring is not enough: the importance of Internet skills for online privacy protection. *Information, Communication & Society, 20*, 1261-1278.

Chellappa, R.K.,& Sin, R.G.(2005). Personalization versus Privacy: An Empirical Examination of the Online Consumer's Dilemma. *Information Technology and Management, 6*(2-3), 181-202.

Chen, A.W., & Chen, C.H. (2016). Research on the influence path of personal information disclosure under government supervision. *Journal of Chongqing University of science and Technology (SOCIAL SCIENCE EDITION), 03,* 31-33.

Chen, H.T., & Chen, W. (2015). Couldn't or Wouldn't? the Influence of Privacy Concerns and Self-Efficacy in Privacy Management on Privacy Protection. *Cyberpsychology, Behavior, and Social Networking, 18*(1), 13-19.

Chen, R. (2013). Living a private life in public social networks: An exploration of member self-disclosure. *Decision Support Systems, 55*(3), 661-668.

Chen, H., Beaudoin, C.E. , & Hong, T. (2017). Securing online privacy: An empirical test on Internet scam victimization, online privacy concerns, and privacy protection behaviors. *Computers in Human Behavior, 70*, 291-302.

Child, J.T., & Petronio, S. (2011). Unpacking the Paradoxes of Privacy in CMC Relationships: The Challenges of Blogging and Relational Communication on the Internet. *Computer-mediated Communication in Personal Relationships*.

Choi, H., Park, J., & Jung, Y. (2018). The role of privacy fatigue in online privacy behavior. *Computers in Human Behavior*, *81*, 42-51.

Culnan, M.J., & Armstrong, P.K. (1999). Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. *Organization Science, 10*(1) , 104-115.

Daniel, J.S. (2008) . *The Future of Reputation.* Yale: Yale University Press.

Dhir, A., Torsheim, T., Pallesen, S., & Andreassen, C.S. (2017). Do Online Privacy Concerns Predict Selfie Behavior among Adolescents, Young Adults and Adults?. *Front Psychol*, *8,* 815.

Du, T. (2018). Annual report on the international frontier of private international law (2016-2017). *International Law studies*, (03), 89-128.

Goffman,E. (1959). *The Presentation of Self in Everyday Life*. Harmondsworth (Penguin): Doubleday.

Haase, A.Q., Ho, D. (2020). Online privacy concerns and privacy protection strategies among older adults in East York, Canada. *Journal of the Association for Information Science and Technology, 71*(9) , 1089-1102.

Hollenbaugh, E.E. (2019). Privacy Management Among Social Media Natives: An Exploratory Study of Facebook and Snapchat. *Social Media + Society, 5*(3), 395-415.

Hozman, D. (2006). *Privacy Lost.* San Francisco: Jossey-Bass.

Laufer, R.S., & Wolfe, M. (1977). Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory. *Journal of Social Issues*, *33*(3) , 22-42.

Lee, H. , Park, H., & Kim, J. (2013). Why do people share their context information on Social Network Services? A qualitative study and an experimental study on users' behavior of balancing perceived benefit and risk. *International Journal of Human-computer Studies, 71*(9), 862-877.

Li, G., & Wang, D.D. (2015). Study on Influencing Factors of users' willingness to disclose personal information on social networking sites: Taking Sina Weibo as an example. *Information work, 36*(1), 35-40.

Lin, A.J., & Cai, M. (2020). Research on the mobile personal data protection under the big-data era. *Modern communication*: *Journal of Communication University of China, 42*(04), 79-83.

Liu, T., & Deng, S.L. (2018). a review of foreign research on privacy paradox. *Journal of Information Resource Management, 8*(02), 104-112.

Lu, J.Y., & Bai, J. (2021). Research on Chinese youth's Internet privacy concerns and their influencing factors -- Based on an empirical survey of 1599 Communist Youth League members. *Journalism Review, 02*, 69-79.

David,S.,&Manuel, C. (1997). The Rise of the Network Society. *Contemporary Sociology*, *26*(6), 725-725.

Dinev, T., & Hart, P. (2011). An extended privacy calculus model for e-commerce transaction. *Information Systems Research, 17*(1), 61 – 80.

Feng, Y., & Xie, W. (2014). Yang Feng and Wenjing Xie. Teens' concern for privacy when using social networking sites: An analysis of socialization agents and relationships with privacy-protecting behaviors. *Computers in Human Behavior, 33*, 153-162.

Malhotr, N.K., Kim, S.S., & Agarwal, J. (2004). Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Information Systems Research, 15*(4), 336-355.

Maslow, A.H. (1943). A theory of human motivation. *Psychological Review, 50*(4), 370-396.
Milne, G.R., & Culnan, M.J. (2004). Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices. *Journal of Interactive Marketing, 18*(3), 15-29.
Mohamed, A. A-A. (2010). Online Privacy Concerns Among Social Networks' Users. *Cross-Cultural Communication,* 6(4), 74-89.
Moon, Y. (2000). Intimate Exchanges: Using Computers to Elicit Self-Disclosure From Consumers. *Journal of Consumer Research, 26*(4), 323-339.
Patricia, A.N., Daniel, R.H., & David, A.H. (2007). The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. *The Journal of Consumer Affairs, 41*(1), 100-126.
Negroponte, N. (1995). *Being Digital.* New York: Knopf Press.
Norsko, A., Wood, E. & Molema, S. (2009). All about me: Disclosure in online social networking profiles: The case of FACEBOOK. *Computers in Human Behavior,* 26(3), 406-418.
Oomen, I., & Leenes, R. (2008). *Privacy Risk Perceptions and Privacy Protection Strategies*. Boston: Springer Press.
Barry Brown(2001). *Studying the internet experienc*e. Retrieved from: https://www.hpl.hp.com/techreports/2001/HPL-2001-49.pdf.
Pentina, I., Zhang, L., Bata, H., & Ying, C. (2016). Exploring privacy paradox in information-sensitive mobile app adoption: Across-cultural comparison. *Computers in Human Behavior, 65*(9), 409 – 419.
Petronio, S., & Altman, I. (2002). *Boundaries of Privacy: Dialectics of Disclosure*. New York: State University of New York Press.
Qin, G.J., & He, D.M. (2011). On the value orientation and dilemma of contemporary privacy ethics. *Journal of Shenyang Institute of Engineering (SOCIAL SCIENCE EDITION), 2011*(3), 9.
Quan-Haase, A., & Ho, D. (2020). Online privacy concerns and privacy protection strategies among older adults in East York, Canada. *Journal of the Association for Information Science and Technology*, *71*(9), 1089-1102.
Sarah, A., Johnson, C.M., & D'Souza, G. (2016). The Complex Web of Values: the Impact on Online Privacy Concerns and Purchase Behavior. *Journal of Electronic Commerce Research, 17*(1), 22-35.
Sayre, S., & Horne, D. (2000). Trading secrets for savings: How concerned are consumers about club cards as a privacy threat?. *ACR North American Advances, 27*, 151-155.
Sheehan, K.B., & Hoy, M.G. (1999). Flaming, complaining, abstaining: how online users respond to privacy concerns. *Journal of Advertising, 28*(3), 37-51.
Shen, Q. (2014). Research on network literacy and network privacy protection behavior: Taking College Students in Shanghai as the research object. *Journalism University,* (05), 110-118.
Shi, S. (2011). *Research on the privacy disclosure behavior of social networking website users: the integration of privacy computing theory and TPB model* (MBA Thesis). Retrieved from Nanjing University database.
Stone, E.F., & Stone, D.L. (1990) . Privacy in organizations: Theoretical issues, research findings, *Research progress in Human Resources Management, 8*(3), 349-411.
Tufekc, Z. (2007). Can You See Me Now? Audience and Disclosure Regulation in Online Social Network Sites. *Bulletin of Science, Technology & Society, 28*(1), 20-36.
Turow, J., & Hennessy, M. (2007). Internet privacy and institutional trust: insights from a national survey. *New media & society, 9*(2), 300-318.
Wang, T., Duong, T.D., & Chen, C.C. (2016). Intention to disclose personal information via mobile applications: A privacy calculus perspective. *International Journal of Information Management, 36*(4), 531-542.
Wu, C.K. (2019). *Research on privacy disclosure intention of social media users from the perspective of privacy fatigue* (Master's thesis). Retrieved from Tianjin Normal University database.
Wu, H.B.,& Zeng, K. (2023). The transformation of the life world and communication behavior from the perspective of the metauniverse. *Journal of Social Sciences*, (01), 187-194.
Xiang, S.J. (2011). *Openness and concealment: Research on privacy in the new media era*. Peking: Intellectual property press.
Xie, W.H., Chang, Q.Q., & Li, Z.S. (2018). Research progress of Internet privacy paradox abroad -- theoretical integration and review. *Modern Intelligence, 38*(11), 136-144.
Xie, W., & Karan, K. (2019). Consumers' Privacy Concern and Privacy Protection on Social Network Sites in the Era of Big Data: Empirical Evidence from College Students. *Journal of Interactive Advertising, 19*(3), 187-201.
Yao, M.Z., Rice, R.E., & Wallis, K. (2007). Predicting user concerns about online privacy. *Journal of the American Society for Information Science and Technology, 58*(5), 710-722.
Young, A.L., & Quan-Haase, A. (2013). Privacy Protection Strategies On Facebook: The Internet privacy paradox revisited. *Information, Communication & Society, 16*(4), 479-500.
Yuan, Y.X. (2019). *Research on media ethics in the era of big data* (Master's thesis). Retrieved from Shanxi University database.
Zhang, Y., & Zhu, Q.H. (2014). Review of foreign research on information privacy. *Library and information work, 58*(13), 140-148.
Zhu, H., Wang, K., Yan, Z. J. & Wu, J. (2017). Research on SNS user privacy paradox based on privacy computing theory. *Journal of information, 36*(02), 134-139.