International Journal of Education and Humanities
ISSN: 2770-6702 | Vol. 17, No. 3, 2024

The Influence of Information Exposure on Teenagers' Privacy Protection Behaviour under the Intelligent Recommendation System

Saiya Cheng*

Journalism, Xiamen University Malaysia, Sepang, Selangor, 43900, Malaysia
* **E-mail:** chengsaiya04@outlook.com

Abstract: This study focuses on the influence of information exposure under an intelligent recommendation system on teenagers' privacy protection behaviour. By employing the Communication Privacy Management (CPM) theory, we examine how information exposure through intelligent recommendation systems influences teenagers' attitudes and actions towards privacy. The results of this study emphasize the need for the CPM advocated by Petronio [1] and the role of various factors in influencing privacy protection behaviour. The study also explores teenagers' privacy protection behaviours on social media. Through quantitative research, this study provides a perspective on the interaction among adolescents' digital literacy, privacy issues and behavioural responses in the context of intelligent recommendation systems.

Keywords: Information Exposure; Privacy Protection Behaviour; Intelligent Recommendation System; Privacy Risk Perception; Privacy Boundary Control; Awareness of Privacy Protection; Communication Privacy Management Theory.

1. Introduction

With the continuous improvement in the accuracy of intelligent recommendation systems and advancements in AI technology, their impact on individual behaviours becomes increasingly profound. For the social media environment, the main function of a recommendation system is to help users make better decisions, overcome data overload and promote content that is more convenient for users [2]. Contemporary recommendation systems anticipate users' future interactions by leveraging historical behavioural data [3]. The primary objective of a recommendation system is to anticipate users' preferences and provide suggestions based on their potential areas of interest. Product descriptions using keywords are recommended with content related to the user's preferred configuration [4]. However, the intelligent recommendation system depends on the user's online behaviour, feedback preferences and other personal information when using social media, which requires the user to sacrifice personal information, which is easy to causes information cocoon and privacy security problems. Numerous social media platforms have implemented intelligent recommendation systems, which employ various techniques like collaborative filtering, content-based filtering, and hybrid approaches to anticipate and suggest items that users are likely to engage with [5]. The primary objective of these systems is to enhance user involvement and satisfaction by presenting content aligned with their interests. For teenagers, this information exposure is frequently influenced by recommendation systems that customize material according to user data. This negative sentiment may encourage users to avoid the risks associated with disclosing personal information to social platforms [6]. To protect their privacy while passively receiving information, they can adopt privacy protection measures, privacy avoidance strategies, or more adaptable defensive approaches based on their algorithmic perception.

According to a new survey of American teens by the Pew Research Center, 2023, teens use such recommendation platforms at a high rate, despite negative headlines and growing concerns about social media's influence on teens. However, some describe the frequency of use of their media platforms as "almost all the time." Research shows that 58% of teens are regular TikTok users. Of those, 17% said they use TikTok almost all the time. In addition to asking teens about their media platform use, the report also shows how much time teens spend online. Nearly half of teens say they use the Internet "almost all the time." Overall, more than 9 in 10 said they use the Internet at least daily. Data privacy company Tsaaro, 2022, in its report on the state of youth data security in the Internet world, highlighted that teens are increasingly sharing personal information on social media sites. According to the DQ Institute, 2023, nearly 70% of children and adolescents worldwide will have been exposed to online risks. Cyber risks vary by age but include the exposure of personal information. The prioritization of user engagement in recommendation systems' algorithms may lead to the promotion of sensational or extreme content, potentially exposing teenagers to harmful or inappropriate material [7].

2. Literature Review

The advent of intelligent recommendation systems has sparked a revolutionary metamorphosis in the digital domain, profoundly impacting users' interactions with online content. These aforementioned systems employ sophisticated algorithms to tailor user experiences by proffering content that aligns with their preferences and behaviours. Recommendation systems belong to the category of information-filtering systems that utilize personalized knowledge-filtering techniques to anticipate an individual's inclination towards a specific item [9]. The utilization of these systems not only enhances user engagement and satisfaction levels but also gives rise to significant privacy concerns, particularly among adolescents. This study investigates the application of intelligent recommendation systems, their impact on teenagers, and the relationship between information exposure and privacy protection behaviours.

2.1. Intelligent Recommendation Systems

These systems employ a combination of techniques, including collaborative filtering, content-based filtering, and hybrid methods, to analyze user data and generate personalized recommendation [5]. Collaborative filtering is widely utilized by platforms like Netflix and Amazon to offer suggestions by examining the behaviour patterns of similar users such as their ratings and purchase history [10]. Nevertheless, the substantial data gathering necessary for the operation of such systems gives rise to notable apprehensions regarding privacy. It is evident that there exists a discrepancy between the data gathered by the intelligent recommendation system and the information users are willing to disclose, particularly regarding usage patterns and feedback. The user's private activities and personal details they prefer to keep confidential might be reflected in this data trail. If the system collects and utilizes this information without the consent or knowledge of the user, it can lead to privacy concerns [11].

2.2. Impact of Intelligent Recommendation Systems on Teenagers

Teenagers are among the most active users of social media and other online platforms, making them particularly susceptible to the influences of intelligent recommendation systems. For example, TikTok, a video recommendation media platform, is very popular among young people. In the United States, approximately 27% of TikTok's user base consists of individuals aged between 13 and 17, while around 41% fall within the age range of 18 to 24. A significant majority, amounting to about 90%, of teenagers and young adults who use this application engage with it daily. Although ByteDance does not disclose specific figures regarding TikTok users under the age of eighteen in their official report, recent nationwide research conducted in China indicates that over half of middle and high school students who access the internet are active users of video-sharing social media platforms [16]. The privacy issue is further intensified when the platform utilizes the user's profile and real-time activities to gather and analyze privacy information of teenage TikTok users, triggering the involvement of the recommendation algorithm [17]. Hence, teenagers must strike a balance between their individual needs and the potential risks associated with divulging personal information within intelligent recommendation systems. This research draws upon Petronio's [20] Communication Privacy Management (CPM) theory and posits that teenagers utilizing such systems will develop diverse strategies for managing their privacy.

2.3. Information Exposure and Privacy Protection Behaviour

There are advantages to sharing information on the Internet, such as fostering and maintaining social connections [12]. Furthermore, utilizing personal data for tracking purposes can enhance website usability, convenience and efficiency; Additionally empowering businesses to personalize services and information [13]. Nevertheless, these benefits also entail risks concerning individuals' privacy. A crucial aspect of safeguarding information privacy is an individual's ability to exercise control over the gathering and dissemination of personal data [14]. Consequently, individuals harbour concerns regarding their online privacy fearing potential misuse of personal data while expressing a desire for greater authority over their online personal information [15]. As a result, managing and protecting one's online privacy has become an integral part of everyday life.

Privacy protection behaviour pertains to particular steps individuals take to guarantee the safety of their data while utilizing computers [16]. By restricting the disclosure of personal information and taking protective behaviours, individuals can effectively shield their online privacy [17].

2.4. Communication Privacy Management Theory (CPM)

According to CPM, individuals believe that they possess their own personal information and hold the authority to control it. This theory emphasizes the various strategies employed by individuals to protect their personal information and maintain their privacy boundaries [18]. Andrews, Walker and Kees [19] explore how young people protect their privacy on social media platforms. Their findings highlight the importance of privacy risk perception in controlling personal information. Based on the theoretical and empirical basis of CPM, this study proposes the following hypotheses.

H1: The level of information exposure on the intelligent recommendation algorithm platform is positively associated with teenagers' privacy protection behaviour.

2.4.1. Privacy Risk Perception

Based on the CPM theory, effective private information management primarily revolves around boundary control. The research acknowledges this perception of risk as a component within the formation of privacy boundaries [20] and recognizes its significance in assessing factors that influence actions taken for safeguarding privacy. In this particular scenario, the perception of privacy risk refers to the anticipated level of potential harm that may arise from disclosing personal information to a recommendation algorithm platform [21]. Thus, we propose the following hypothesis.

H2a: Information exposure on the intelligent recommendation algorithm platform is positively associated with the perception of privacy risks.

H2b: Enhancing juvenile's perception of privacy risks has a positive impact on their engagement in privacy protection actions.

2.4.2. Privacy Boundary Control

The metaphorical boundaries of privacy serve as a means to establish legitimate possession. The thickness of these boundaries reflects the level of "boundary permeability," which determines the extent to which private information is revealed based on the discretion of the owner in granting or denying access [22]. Child and Agyeman-Budu [23] investigated the correlation between intermediary latency, policy ambiguity utilization, and privacy management on Facebook to analyze the fine line between border permeability and control. In particular, the research discovered that individuals employ deliberately vague details (managing levels of involvement and shared ownership) as a means to safeguard their privacy while engaging on social media platforms when they harbour concerns about lurking intermediaries online, so we assume.

H3a: There exists a positive correlation between the extent of information exposure on the intelligent recommendation algorithm platform and teenagers' ability to control their privacy boundaries.

H3b: The enhancement of teenagers' privacy boundary control has a positive impact on their engagement in privacy

protection actions.

2.4.3. Awareness of Privacy Protection

The awareness of privacy protection is important for ensuring the safety of teenagers' online activities. Paying attention to media news or personal experiences of privacy exposure can increase awareness. Studies in recent years has emphasized that privacy education can improve people's awareness of privacy protection. Martin and Nissenbaum [24] emphasized the importance of contextual integrity, suggesting that awareness of privacy protection must proceed within the specific data practices and norms of intelligent recommendation systems to be truly effective. Additionally, Shin and Valente [25] showed that privacy literacy programs significantly improved teenagers' understanding of digital privacy and their ability to manage privacy Settings. Xu, Gupta and Chen, [20] found that individuals with higher awareness are more vigilant about their online activities and more likely to engage in privacy-preserving actions. Given these findings, it is hypothesized that.

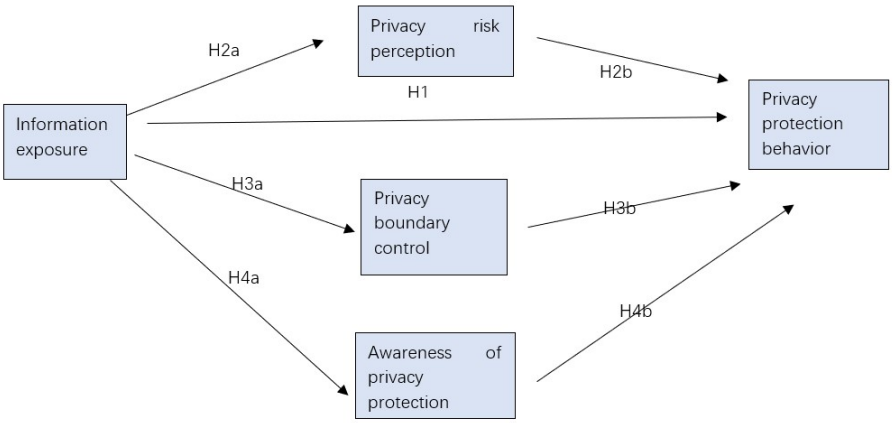
H4a: There is a positive correlation between the extent of information exposure on the intelligent recommendation algorithm platform and teenagers' awareness of privacy protection.

H4b: The enhancement of teenagers' awareness of privacy protection positively influences their engagement in privacy protection actions.

2.4.4. Gaps

Despite the proliferation of intelligent recommendation systems on social media platforms and the profound impact these systems have had on teens, there are some limitations to existing research. The rapid development of intelligent recommendation systems means that teenagers are constantly being exposed to new types of personalized content [26]. Therefore, this study can contribute to more communication research and explore the influence of information exposure on teenagers' behaviour.

Table 1. Hypothesis model



3. Research Method

3.1. Questionnaire Development

In this study, the CPM model and related research of Krasnova, Spiekermann, Koroleva and Hildebrand [27] on privacy protection behaviour were mainly referred to in the selection of research model variables. This study provides a comprehensive overview of the impact of information exposure on privacy protection behaviours among teenagers, as well as the influence of privacy risk perception, privacy boundary control, and awareness of privacy protection on such behaviours within the framework of CPM theory. The variables tested in this study are operationally defined and the scale sources are shown in Table 2 below.

Table 2. Variable definitions and sources

Variables	Definition	Sources
Information Exposure	Information Disclosure pertains to the aggregate of diverse information presented or suggested by the intelligent recommendation system that an individual receives while utilizing the said system.	Adapted from Spiekermann [28].
Privacy Risk Perception	Privacy risk perception pertains to an individual understanding and awareness of the potential dangers and vulnerabilities that their personal data might encounter while utilizing intelligent recommendation systems or other internet-based services.	Adapted from Child, Agyeman-Budu and Esther [22].
Privacy Boundary Control	Privacy boundary control pertains to individuals' capacity to establish and regulate limits on information, ensuring the preservation of their privacy during the exchange and safeguarding of data.	Adapted from Child, Agyeman-Budu and Esther [22].
Awareness of Privacy Protection	Awareness of privacy protection pertains to an individual apprehension regarding matters of privacy and their understanding of measures taken for safeguarding privacy.	Adapted from Spiekermann [28].
Privacy Protection Behaviour	Privacy preservation behaviour pertains to the practical measures individuals adopt in safeguarding their personal data and privacy while utilizing intelligent recommendation systems or other online services regularly.	Adapted from Child, Agyeman-Budu and Esther [22].

3.2. Data Collection and Samples

The study was conducted in 2024 at a public middle school located in northern China, utilizing an online questionnaire to gather empirical data for the research project. The online questionnaire was approved by the principal and 488

responses were received, of which 414 were valid (valid N=414). Online questionnaires are a suitable research tool due to their high convenience and ease of management, resulting in reduced costs [29]. Meanwhile, online questionnaires can better safeguard the anonymity of participants [30], particularly when inquiring about privacy concerns.

The questionnaires were selected based on established principles. For online questionnaires, those with a response time of less than 90 seconds were excluded. Among the valid study responses collected, only 37.2% of the students reported receiving training or education on personal information protection, indicating that a majority (62.8%) had limited knowledge in this area. Regarding personal information breaches or privacy violations, approximately 30% of students believed they had experienced such incidents. The subjects of the questionnaire are all high school students, and at the same time, the teenagers who are subject to privacy security crises are certified.

3.3. Validity Analysis

The KMO value of the scale data was 0.908, which is greater than the recommended threshold of 0.6, as evidenced by the data presented in the table above. Furthermore, the Bartley ball test was conducted with a significance level of $P < 0.05$, and it demonstrated that the scale survey data is highly suitable for factor analysis. The results of the factor analysis are shown in Table 3.

Table 3. Factor Analysis

KMO and Bartlett's Test		
Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.908
Bartlett's Test of Sphericity	Approx. Chi-Square	4082.163
	df	105
	Sig.	.000

Table 4. Total Variance Explained

	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
Component	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	6.106	50.886	50.886	6.106	50.886	50.886	2.433	20.273	20.273
2	1.478	12.313	63.199	1.478	12.313	63.199	2.419	20.155	40.429
3	1.034	8.616	71.814	1.034	8.616	71.814	2.323	19.359	59.788
4	.772	6.434	78.249	.772	6.434	78.249	2.215	18.461	78.249
5	.519	4.325	82.574						
6	.427	3.559	86.132						
7	.389	3.243	89.375						
8	.348	2.898	92.273						
9	.267	2.222	94.495						
10	.257	2.139	96.634						
11	.235	1.959	98.593						
12	.169	1.407	100.000						
Extraction Method: Principal Component Analysis.									

The variance contribution rate analysis table reveals that a total of four primary factors can be extracted from the 12 questions with high reliability. These factors collectively account for 78.249% of the information in the overall table, surpassing the threshold of 60%. Hence, these extracted common factors are highly effective in fully capturing and explaining the information contained within the original scale.

Table 5. Rotated Component Matrix

	Component			
	1	2	3	4
You have concerns about the way media platforms collect and use your personal information on the Internet.	.858			
When you realize that a media platform is collecting and using your personal data, you feel very insecure.	.803			
You know that your personal data may be used inappropriately by the platform.	.730			
Privacy is important to you.		.842		
You think it is important to read the privacy policy of the recommended platform carefully.		.836		
You think it's important to "control who can access the personal privacy you put online".		.748		
You are concerned that your personal data may be provided to unknown individuals or institutions.			.821	
You believe that the disclosure of personal privacy will cause loss..			.810	
You understand the negative impact that disclosure of personal information may have on personal privacy, financial security and personal image.			.718	
You will review and update your privacy settings regularly.				.830
You will often clear your browsing history on the platform.				.816
You will choose to set up a private account on the recommended platform to control who can see the information.				.715
Extraction Method: Principal Component Analysis. Rotation Method: Varimax with Kaiser Normalization.				

Based on Table 5 Rotated Component Matrix provided, we can analyze the factor structure of the items related to privacy concerns and behaviours among adolescents.

3.4. Reliability Analysis

Table 4 presents the results of the exploratory factor

analysis with Varimax rotation, revealing four extracted factors. To assess the reliability of these factors, we conducted a Cronbach α coefficient test (refer to Table 6). In this study, Cronbach's α reliability coefficient was employed to assess the reliability of privacy risk perception, privacy boundary control, privacy protection consciousness, and privacy protection behaviour.

Table 6. Reliability coefficient

Factor	N of Items	Cronbach α
Information Exposure	3	.87
Privacy Risk Perception	3	.86
Privacy Boundary Control	3	.80
Awareness of Privacy Protection	3	.87
Privacy Protection Behaviour	3	.86

All factors demonstrate good to high reliability, indicating that the items within each factor consistently measure the same construct. Cronbach's α values above 0.8 suggest strong internal consistency among the items.

3.5. Current Situation Analysis

The survey instruments include measures to assess the following topics :(1) vulnerability to information exposure; (2) information disclosure brings benefits; (3) privacy risk perception; (4) privacy boundary control; (5) awareness of privacy protection; (6) privacy protection behaviour. Participants were requested to indicate the perceived likelihood of each risk occurrence specifically to themselves. All items were assessed using a 5-point Likert scale, ranging from 1 = 'strongly disagree' to 5 = 'strongly agree'. Four items were aggregated for subsequent analysis (α = .85). The results of the analysis are presented in Table 7.

Table 7. Status Analysis

Factor	Mean	S.D.	T	P
Information Exposure	4.08	1.01	21.697	<0.001
Privacy Risk Perception	3.85	.98	17.597	<.001
Privacy Boundary Control	3.81	.81	20.458	<.001
Awareness of Privacy Protection	4.34	.77	35.575	<.001
Privacy Protection Behaviour	3.97	.79	25.065	<.001

Note: Since it is a 5-degree Likert scale, a score of 3 indicates neutrality, so the test value is 3.

The table clearly illustrates that the average scores for the five dimensions of information exposure, privacy risk perception, privacy boundary control, privacy protection awareness, and privacy protection behaviour are 4.08, 3.85, 3.81, 4.34, and 3.97 respectively. All these scores significantly surpass the neutral value of 3 points. Moreover, the P-values obtained from single-sample T-tests are all <0.05, indicating that this survey reveals a positive outlook among teenagers regarding their perceptions of privacy risks, control over personal boundaries, consciousness about protecting their own privacy rights as well as actual behaviours to safeguard their privacy.

Below is a detailed Table 8 summarizing the descriptive statistics of key survey items.

Table 8. Descriptive Statistics

Factor	Mean	S.D.
You believe that the disclosure of personal privacy will cause loss;	4.02	1.087
You are concerned that your personal data may be provided to unknown individuals or institutions;	3.96	1.245
You understand the negative impact that disclosure of personal information may have on personal privacy, financial security and personal image	4.09	1.089
You know that your personal data may be used inappropriately by the platform	3.58	1.180
You have concerns about the way media platforms collect and use your personal information on the Internet	3.94	1.083
When you realize that a media platform is collecting and using your personal data, you feel very insecure	4.03	1.071
You will review and update your privacy settings regularly	3.85	.925
You will choose to set up a private account on the recommended platform to control who can see the information	3.80	1.005
You will often clear your browsing history on the platform	3.79	.932
Privacy is important to you. How important privacy is to you	4.52	.789
You think it is important to read the privacy policy of the recommended platform carefully	4.31	.859
You think it's important to "control who can access the personal privacy you put online".	4.19	.927
Read their privacy policy carefully	3.94	.894
Proactively change privacy settings	3.91	.916
Turn off web tracking	4.07	.857

3.6. Findings

The regression model is analyzed to examine the hypothetical relationship between variables. Specifically, this study posits that privacy risk perception, privacy boundary control, and privacy protection awareness serve as mediating factors influencing the impact of information exposure on adolescents' privacy protection behaviour. To assess the mediation effect of these three variables, a parallel mediating model was employed in this study. Information exposure is considered the independent variable (X), while privacy risk perception (M1), privacy boundary control (M2), and privacy protection awareness (M3) are regarded as mediating variables, with privacy protection behaviour being the dependent variable (Y). Table 9 and 10 illustrates the mediating effects of privacy risk perception, privacy boundary control, and privacy protection awareness on information exposure and teenagers' privacy protection behaviours.

1) Information Exposure(X) and Privacy Protection Behavior(Y)

Table 9. The model summary of the Information Exposure (X) and Privacy Protection Behavior(Y)

Model Summary	
R	0.7596
R-squared	0.5770
MSE	0.2650
F	139.4756
df1	4
df2	409
p-value	<0.001

The correlation coefficient (c=0.857) indicates a significant positive association between information exposure (X) and

privacy protection behaviour (Y), with a significance level of 0.017 ($p < 0.001$). This finding suggests that higher levels of information exposure are linked to stronger privacy-protecting behaviours among adolescents.

2) Information Exposure(X) and Privacy risk perception(M1)

Table 10. The model summary of the Information Exposure (X) and Privacy Risk Perception (M1)

Model Summary	
R	0.6654
R-squared	0.4428
MSE	0.5399
F	327.3590
df1	1
df2	412
p-value	<0.001

The correlation coefficient between information exposure (X) and privacy risk perception (M1) was a1=0.644, and the significance level was $p < 0.001$. This suggests a modest positive correlation.

3) Information Exposure(X)and Privacy boundary control(M2)

There is a moderate positive correlation between information exposure (X) and privacy boundary control (M2), the correlation coefficient is a2=0.376, the significance level $p < 0.001$. This suggests that higher information exposure leads to enhanced privacy boundary control for adolescents.

Table 11. The model summary of the Information Exposure(X)and Privacy boundary control(M2)

Model Summary	
R	0.45
R-squared	0.2025
MSE	0.5208
F	104.6383
df1	1
df2	412
p-value	<0.001

4) Information Exposure(X) and Awareness of Privacy protection(M3)

Table 12. The model summary of Information Exposure（X） and Awareness of Privacy protection（M3）

Model Summary	
R	0.5741
R-squared	0.3296
MSE	0.3956
F	202.5319
df1	1
df2	412
p-value	<0.001

The correlation between information exposure (X) and privacy protection awareness was a3=0.434 ($p < 0.001$), which was statistically significant. This showed a strong positive correlation, suggesting that greater information exposure increased adolescents' awareness of privacy issues.

Privacy protection behaviour (Y) and privacy risk perception (M1), privacy boundary control (M2) and privacy awareness (M3).

Table 13. Mediating effect

	Effect	BootSE	BootLLCI	BootULCI	Effect Size
TOTAL	.2816	.0505	.1874	.3852	0.766467
M2	.1689	.0292	.1134	.2283	0.459717
M3	.1555	.0362	.0913	.2328	0.423244

Although the perception of privacy risk (M1) negatively influences privacy protection behaviour, it is not statistically significant ($\beta = -0.0664$, $p > 0.05$). Furthermore, the confidence interval of M1 includes zero, indicating that M1 does not have a mediating effect. Privacy boundary control (M2) significantly and positively affects privacy protection behavior ($\beta = 0.4721$, $p < 0.001$). The confidence interval of M2 does not include zero, suggesting that M2 has a mediating effect and supports hypothesis H3b. Privacy protection awareness (M3) significantly and positively impacts privacy protection behaviour ($\beta = 0.3586$, $p < 0.001$). The confidence interval of M3 does not contain zero, indicating that M3 has a mediating effect and supports hypothesis H4b.

4. Discussion

The findings of this study offer support for the application of CPM theory in comprehending teenagers' privacy behaviour. The strength of the theory lies in its emphasis on individual autonomy in managing personal information. These measures have the potential to enhance teenagers' capacity to navigate the digital environment by implementing enhanced security measures [31]. To effectively implement CPM, educational measures are necessary to enhance teenagers' awareness of privacy and their ability to establish privacy boundaries. However, the limited influence of privacy risk perception on privacy protection behaviour. This result indicates that although teenagers may recognize the risks associated with their privacy, this recognition alone does not necessarily translate into proactive protective actions. This finding highlights the need for further research into determining factors that influence the translation of perceived risk into actionable behaviours, such as exploring self-efficacy and perceived control over personal information.

5. Conclusion

This study's primary objective is to investigate the impact of information exposure within intelligent recommendation systems on teenagers' privacy protection behaviours. To achieve this objective, this study utilized the CPM theory as a theoretical framework. Through investigation and data analysis, the research results show that there is a significant correlation between the four variables of adolescents' information disclosure, privacy risk perception, privacy boundary management, awareness of privacy production and the privacy protection behaviours taken by adolescents. There is a direct correlation between information exposure and the

adoption of privacy-protecting behaviors by adolescents. More information exposure is associated with increased privacy risks perception, increased personal boundary management, and increased awareness of privacy production. These mediating factors significantly affect teenagers' privacy protection behaviours.

This study's results have some practical implications for policymakers and educators. Integrate these measures into academic teaching guidelines to ensure that students acquire the basic competencies to protect themselves in the digital age. In the process of developing an intelligent recommendation system, developers should attach great importance to the protection of user privacy. By ensuring transparency in data collection and use, developers empower users to make informed choices regarding privacy.Despite this study's findings, the study has several limitations. First, using horizontal designs limits our ability to establish causal relationships between variables. Therefore, longitudinal studies are warranted to investigate how privacy behaviours evolve with continued exposure to intelligent recommendation systems. Second, the reliance on self-reported data in this study may introduce social expectation bias. Future research could incorporate behavioural measures of privacy protection to provide a more objective assessment of privacy behaviour.

References

[1] Petronio, S. (2002). Boundaries of Privacy: Dialectics of Disclosure. State University of New York Press, Albany, NY.

[2] Zaman, S., Alhazmi, K., Aseeri, M. A., Ahmed, M. R., Khan, R. T., Kaiser, M. S., & Mahmud, M. (2021). Security threats and artificial intelligence based countermeasures for internet of things networks: a comprehensive survey. Ieee Access, 9, 94668-94690.

[3] Shu, K., Sliva, A., Wang, S., Tang, J., & Liu, H. (2017). Fake news detection on social media: A data mining perspective. ACM SIGKDD explorations newsletter, 19(1), 22-36.

[4] Umamaheswari, D. D. (2024). Role of Artificial Intelligence in Marketing Strategies and Performance. Migration Letters, 21(S4), 1589-1599.

[5] Adomavicius, G., & Tuzhilin, A. (2005). Toward the next generation of recommender systems: A survey of the state-of-the-art and possible extensions. IEEE transactions on knowledge and data engineering, 17(6), 734-749.

[6] 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.

[7] Deogracias A. Danah Boyd: It's Complicated: The Social Lives of Networked Teens: Yale University Press, New Haven, Connecticut, 2014, pp. 296, ISBN 973-0-300-16631-6[J]. 2015.

[8] Moscardelli, Deborah M., and Richard Divine. "Adolescents' concern for privacy when using the Internet: An empirical analysis of predictors and relationships with privacy-protecting behaviors." Family and Consumer Sciences Research Journal 35.3 (2007): 232-252.

[9] Naslund, J. A., Bondre, A., Torous, J., & Aschbrenner, K. A. (2020). Social media and mental health: benefits, risks, and opportunities for research and practice. Journal of technology in behavioral science, 5, 245-257.

[10] Koren, Y., Bell, R., & Volinsky, C. (2009). Matrix factorization techniques for recommender systems. Computer, 42(8), 30-37.

[11] Wang, J., & Xie, J. (2023). Exploring the factors influencing users' learning and sharing behavior on social media platforms. Library Hi Tech, 41(5), 1436-1455.

[12] Gibbs, J. L., Ellison, N. B., & Lai, C. H. (2011). First comes love, then comes Google: An investigation of uncertainty reduction strategies and self-disclosure in online dating. Communication Research, 38(1), 70-100.

[13] Boerman, S. C., Kruikemeier, S., & Zuiderveen Borgesius, F. J. (2017). Online behavioral advertising: A literature review and research agenda. Journal of Advertising, 46(3), 363-376.

[14] Baruh, L., Secinti, E., & Cemalcilar, Z. (2017). Online privacy concerns and privacy management: A meta-analytical review. Journal of Communication, 67(1), 26-53.

[15] Smit, E. G., Van Noort, G., & Voorveld, H. A. (2014). Understanding online behavioural advertising: User knowledge, privacy concerns and online coping behaviour in Europe. Computers in Human Behavior, 32, 15-22.

[16] Milne, G. R., Labrecque, L. I., & Cromer, C. (2009). Toward an understanding of the online consumer's risky behavior and protection practices. Journal of Consumer Affairs, 43(3), 449-473.

[17] Andrews, J. C., Walker, K. L., & Kees, J. (2020). Children and online privacy protection: Empowerment from cognitive defense strategies. Journal of Public Policy & Marketing, 39(2), 205-219.

[18] Omar, B., & Dequan, W. (2020). Watch, share or create: The influence of personality traits and user motivation on TikTok mobile video usage. International Journal of Interactive Mobile Technologies, 14(4), 121-137. doi: 10.3991/IJIM.V14I04.12429

[19] Milne, G. R., Labrecque, L. I., & Cromer, C. (2009). Toward an understanding of the online consumer's risky behavior and protection practices. Journal of Consumer Affairs, 43(3), 449-473.

[20] Indrawan, D., Yorman, Y., Stiadi, M., Hendayani, N., & Al-Amin, A. A. (2023). Revolutionizing social media marketing through AI and automation: an in-depth analysis of strategies, ethics, and future trends. International Journal of Humanities, Social Sciences and Business (INJOSS), 3(1), 22-45.

[21] Xu, H., Gupta, S., & Chen, W. (2022). Examining the impact of privacy education and awareness on protective behaviors: A quantitative analysis. Journal of Information Privacy and Security, 18(1).

[22] Wisniewski, P. J., Vitak, J., & Hartikainen, H. (2022). Privacy in adolescence. In Modern socio-technical perspectives on privacy (pp. 315-336). Cham: Springer International Publishing.

[23] Child, J., & Agyeman-Budu, E. A. (2010). Blogging privacy management rule development: The impact of self-monitoring skills, concern for appropriateness, and blogging frequency. Computer in Human Behavior, 26(6), 957-963.

[24] Martin, K. D., & Nissenbaum, H. (2020). Privacy as contextual integrity. Washington Law Review, 95(1), 463-506.

[25] Shin, D., & Valente, T. (2020). The effect of digital literacy on privacy concerns and behaviors. Telematics and Informatics, 50, 101396.

[26] Vespoli, G., Taddei, B., Imbimbo, E., et al. (2024). The concept of privacy in the digital world according to teenagers. Journal of Public Health (Berlin). https://doi.org/10.1007/s10389-024-02242-x

[27] Krasnova, H., Spiekermann, S., Koroleva, K., & Hildebrand, T. (2010). Online social networks: Why we disclose. Journal of Information Technology, 25, 109-125.

[28] Spiekermann, S. (2007). Perceived control: Scales for privacy in ubiquitous computing. In Digital Privacy (pp. 289-304). Auerbach Publications.

[29] Garrett, R., & Wrench, A. (2008). Connections, pedagogy and alternative possibilities in primary physical education. Sport, Education and Society, 13(1), 39-60.

[30] Joinson, A. (1999). Social desirability, anonymity, and Internet-based questionnaires. Behavior Research Methods, Instruments, & Computers, 31(3), 433-438.

[31] Hantrais, L., Allin, P., Kritikos, M., Sogomonjan, M., Anand, P. B., Livingstone, S., ... & Innes, M. (2021). Covid-19 and the digital revolution. Contemporary Social Science, 16(2), 256-270.