VNU Journal of Economics and Business

Journal homepage: https://jeb.ueb.edu.vn

Original Article

Privacy Risk Awareness and Intent to Disclose Personal Information of Users Using Two Social Networks: Facebook and Instagram

Dinh Tien Minh*, Pham Thi Truc Ly, Nguyen Thi Ngoc Duyen

School of International Business and Marketing - University of Economics Ho Chi Minh City, No. 279 Nguyen Tri Phuong, Ward 5, District 10, Ho Chi Minh City, Vietnam

Received: November 11, 2022
Revised: December 1, 2022; Accepted: December 25, 2022

Abstract: The research focuses on the perception and awareness of privacy risks to disclose users' personal information on two social networking platforms, Facebook and Instagram. The data was collected from 428 Facebook and Instagram users aged from 15 to 29 years old by an online questionnaire. The Structural Equation Model (SEM) was used to analyze the relationships in the research model supported by SPSS 20.0 and AMOS 24.0 software. Results indicate that if user trust or confidence is high in social networking sites such as Facebook and Instagram, the perception of user privacy risk is low. This result is beneficial for the researcher to have a fresh look at consumer behavior. For businesses, it takes a long time to develop a product that will gain the trust of customers. They must ensure that their products are as risk-free as possible in order to maintain consumer trust, because when consumers choose to trust, they always expect the product's risk to be as low as possible or zero. From the research results, it is possible to make suggestions for solutions to overcome the perceived problem of users in disclosing personal information on social networks in general. And it clearly shows that the factors that motivate online social media users to disclose personal information are extremely different.

Keywords: Facebook, Instagram, personal information disclosure, social networks, user awareness, user consciousness.

* Corresponding author
E-mail address: dinhtienminh@ueh.edu.vn
https://doi.org/10.57110/vnujeb.v2i6.133

1. Introduction

Social network sites provide their users with the functionalities of creating profiles, connecting with others, and interacting (Boyd & Ellison, 2007; Loiacono et al., 2012). Social network site providers such as Instagram and Facebook have grown rapidly through real-time communication and information sharing. As of the first quarter of 2022, Facebook reports having 2.936 billion monthly and 1.960 billion daily active users on average, an increase of 33.60% compared to 2018 (Statista.com, 2022).

Studies on social network sites have shown that privacy concerns negatively affect users' disclosing intention to disclose personal information but have no significant impact on actual disclosing behaviors (Joinson et al., 2010; Norberg et al., 2007). Kim and Kim (2020) explored the formation mechanisms of users' disclosing behaviors from the perspectives of the privacy paradox (benefit and risk). Kroll & Stieglitz (2021) found that digital nudges may have a converse effect, meaning that reminders to change privacy settings trigger privacy concerns. The identified nudges aiming at a higher privacy awareness do not yield clear results on self-disclosure. Following the previous empirical research, we will cast light on the impact of the privacy risk awareness of the users themselves on their intention to disclose personal information on two major social networking sites, Facebook and Instagram. In line with the Theory of Perceived Risk (TPR) (Bauer, 1960) and Theory of Planned Behavior (TPB) (Ajen, 1991), a new relationship between variables will be discovered.

This research offers contributions to the theory of consumer behavior on social network sites concerning disclosing behaviors; and on the practical side, the results of this study will support businesses to build products and marketing campaigns with low risk to get more trust of customers in the social network sites.

In this paper, we begin with a review of the two theories above-mentioned and previous studies to develop a hypothesis and a research model. Next, we present the methodology and the experiments that examine this relationship among variables. The study establishes how the perception of privacy risk positively affects the intent to disclose personal information with the other constructs as trust, personalization, knowledge and privacy invasion experience. The research results are shown in the fourth part. Finally, we discuss the theoretical and practical contributions.

2. Hypothesis and research model

2.1. Theory of Perceived Risk (TPR)

According to Bauer (1960), perceived risk is defined as consisting of two main components: the probability of a loss and the subjective feeling of a bad outcome. The TPR developed by Bauer states that the behavior of consuming technology products influenced by perceived risk includes two elements: Perceived Risk associated with Product/Service (PRP) and Perceived Risk associated with the context of online Transaction (PRT). The PRP represents customers' concerns about loss of functionality, loss of finance, loss of time, and loss of opportunity when using technology products/services, while the PRT are the risks that consumers may face when transacting by electronic means; such as confidentiality, safety, and total risk when making transactions.

2.2. Theory of Planned Behavior

The Theory of Planned Behavior (TPB) invented by Ajzen in 1991 is an extension of the Theory of Reasoned Action (TRA) developed by Ajzen and Fishbein in 1975. TPB theory overcomes the limitation of TRA when predicting behavior that people cannot control. Ajzen suggested that perceived behavioral control influences an individual's intention to perform a behavior and he added this factor to the model. The model includes three variables: Attitude, Subjective Norm, and Perceived behavioral control that have a direct impact on behavioral intention.

Perceived behavioral control was also predicted to have a direct influence on actual behavior along with behavioral intention. Perceived behavioral control refers to available resources, skills, and opportunities, as well as an individual's own perception of the importance of achieving results.

2.3. Research model and hypotheses

The concept of level of trust refers to the degree to which an organization is deemed trustworthy and benevolent by consumers and possesses integrity as well as essential skills and competencies (Caldwell & Clapham, 2003; Mayer & Davis, 1999). According to a research paper of Michaelidou and Micevski (2019) on Consumer Ethical Perceptions of Social Media Analysis Methods: Potential Risks, Benefits, and Outcomes state that: the lower the trust level, the higher the awareness of disregard for information disclosure on social networks. This is like the Social Exchange Theory (SET) commonly used to form the concept of trust, focusing on the rules of exchange, in which the interactions between one party are conditional and dependent on the actions of the other party (Cropanzano & Mitchell, 2005). In addition, lack of trustworthiness affects a consumer's decision to provide fake information in an act of protection or retaliation. Consumers expect and trust organizations to protect their information (Punj, 2017).

H1: High user trust in the media has a positive impact on Facebook and Instagram users' perceptions of privacy risk.

Interpersonal relationships are based on a subjective evaluation of benefits and costs (Homans, 1958, p. 606). The Privacy Calculus Theory argues that some users feel that the returns for disclosure offset the risk of their privacy being compromised (e.g., Dinev & Hart, 2006; Culnan & Armstrong, 1999). The research found that people are willing to sacrifice the safety of their personal information if the perceived benefits outweigh the costs (for an overview, see Beldad et al. (2011), p. 225), and despite privacy concerns, adolescents are particularly receptive to the potential benefits of disclosing personal information (Christofides et al., 2009, p. 342).

Benefits that are associated with the disclosure are plentiful: enjoyment (e.g., Krasnova et al., 2009), self-presentation (e.g., Boyd, 2009) and the ability to maintain social ties (e.g. Ellison et al., 2007).

H2: Perceived benefits have a positive effect on the intention to disclose personal information on Facebook and Instagram.

In the first study "Personal Information Sharing Habits", habits have been found to impact behavior beyond other factors (Burton-Jones & Hubona, 2006), and are a stronger predictor of behavior than Intention (De Bruijn et al., 2008; Kremers & Brug, 2008, Limayem et al., 2007; Polites & Karahanna, 2012). The second research paper has shown that habits apply well to online social networking (OSN) usage behavior, and habits can trigger intention automatically. Presenting with Lankton et al., (2012), OSNs' conduct is influenced by their behaviors (the other social networks like Facebook or Instagram are used to replace them in this research).

The relationship between habit and continuation purpose is explained by using habit theory (Lankton et al., 2012). Intention and users can be automatically triggered by habits (Ajzen, 2002, p. 119) and elicit strong feelings of friendliness against such behaviors based on previous habitual practices, thus increasing the desire to continue the activity (Ellison et al., 2007; Beldad, de Jong, & Steehouder, 2011).

H3: Intention to disclose personal information on Facebook and Instagram has increased as a result of habit.

The article by Li et al. (2020) writes about "Voluntary and mandatory provisioning: Personal information disclosed on social networking sites" claiming personalization impacts positively come to social media users' risk perception. The research shows that personalized services have significant security implications because the premise of those

services is the collection of large amounts of personal data (Kobsa, 2007). An individual can provide important information such as name and contact information to a website. These disclosures may lead to unwanted marketing, advertising, price discrimination, and unauthorized access (McKnight et al., 2002).

H4: Personalization positively affects Facebook and Instagram users' perception of privacy risks.

Based on the research, "Understanding third-party perceptions of privacy risks on the Internet", by Chen and Atkin (2021), it is necessary to develop the issue of how an understanding of social media users of Facebook and Instagram impacts perceptions of privacy risks and disclosure of personal information and cognitive knowledge, indicating an individual's level of familiarity with an issue (Nunes et al., 2011). Individuals gain knowledge from the media, education, and personal experience. A person perceives that if the risk that his or her private information or personal information being disclosed through the media will negatively affect them, they tend to limit the disclosure of their personal information or use fake information to protect themselves from the risk and vice versa. Framing a message, status bias, anchor effects, positive bias or peer pressure (overwhelming impact) can also lead to disclosure decisions. Therefore, the knowledge and understanding of social media users about privacy risk are the factors that adjust the user's behavior to match the perception of the level of risk they consider happening to themselves.

H5: Users' perceptions of privacy risks on Facebook and Instagram are positively influenced by user knowledge.

Through reference studies, privacy concerns are negatively correlated to disclose personal information, but this effect varies in different contexts. Beuker (2016) established that privacy concerns have less influence on the willingness to disclose personal information in Dutch Facebook users. Contrarily, in a very recent study, Zhang and Fu (2020) found that the volume, intimacy, and honesty of self-disclosure on social networking sites have been adversely associated with privacy concerns. According to Beldad et al. (2011), the threats associated with personal information exposure are many, and the risks vary depending on the quantity and quality of information revealed. Finally, OSN users are becoming more mindful that the details they freely share can be misused by crooks, stalkers, bullies, or even one's friends (e.g., Staksrud & Livingstone, 2009; Saunders & Zucker, 1999). According to Youn (2005), "As teen privacy threats became more serious, they became less able to provide personal information to a website".

H6: The perception of privacy threats has a negative impact on personal information disclosure.

A large-scale investigation was conducted and it discovered that, as opposed to those who have never had their privacy violated, those who have had their privacy violated pay more attention to information privacy and have a more negative attitude when asked to provide personal information. Several typical surveys found: the attitude toward private information is influenced by prior experiences (Xu, 2007) and, when people who have previously been subjected to a breach of privacy are confronted with a similar situation, their previous encounters are likely to affect their potential perceptions (Zhao et al., 2012). As a result, people who have been subjected to privacy invasions are more concerned with privacy violations than those who have not.

H7: Experiences of invasions of privacy have a major effect on risk perceptions.

One kind of private security is a privacy policy which is described as a system that informs users of their options for how the collected information is used, that protections are in place to protect the information from deletion, abuse, or alteration, and how users can update or fix any incorrect information (Hui et al., 2007). On this basis, Xu et al. (2011) and other researchers (Chang et al., 2018; Culnan & Armstrong, 1999; Culnan & Bies, 2003; Xu et al., 2008.) discovered that users' perceived

privacy threats are reduced when privacy policies are perceived to be successful. Furthermore, Culnan & Armstrong (1999), Van Slyke et al. (2006) concluded that providing a privacy policy to consumers through an entity limits users' self-limitation in sharing personal information.

H8: The perceived effectiveness of a privacy policy reduces the intention to disclose personal information on Facebook and Instagram.

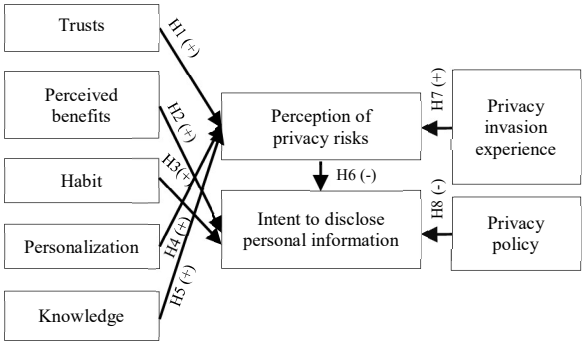

Figure 1: Proposed research model
Source: Author's proposal.

3. Methodology and data

3.1. Pilot research

In this study, qualitative research is represented by in-depth interviews with 8 people, including one person who is an expert on privacy issues. The remainder were ordinary users of the social networks Facebook and Instagram, interviewed using a set of questionnaires to uncover new factors influencing information disclosure and perceived risk about information disclosure privacy as well as adjusting and supplementing the scales.

3.2. Official research

3.2.1. Sampling method

In this study, the sampling method chosen is convenience sampling. The data was collected through the form of submitting an online survey form.

The study was conducted with all Facebook and Instagram users aged 15-29 years by online survey with a questionnaire built on the Likert scale from Likert 1 to Likert 7, sample size 400. The data were processed on SPSS 20.0 and Amos 24.0 software. The research methods used in this study are Cronbach's Alpha reliability test EFA factor discovery, CFA confirmatory factor analysis, and SEM structural model analysis.

3.2.2. Sample size

Method of calculating the number of samples by age clusters: Regarding the age to be surveyed, the age group of 15 to 29 were divided into the following ranges: From 15 to 19, from 20 to 24, and from 25 to 29.

The method of calculating the number of samples is accurate and the number of people of each age is divided according to the recent total report on the population of Vietnam in 2019. In 2019, Vietnam's population was 96,462,108 people. Because the gaps need to be surveyed, groups focus on only 3 main groups stretching from 15 to 29 years old. The number of samples is as follows:

$$n = \frac{N}{(1+N*e^2)}$$

n: Number of sample members to be determined for the investigation study. N: The total number of samples. e: Standard deviation and e = 0.05.

N: Vietnam's total population will be between 15 and 29 years old in 2019. And N = 22,361,416 people.

Based on formula (1), the sample size is 400.

The scales are measured by the seven-point interval scale and the observational variables are based on various authors, such as *Trust* from Krasnova et al. (2010); *Perception of Benefit* from Ellison et al. (2006), and Krasnova et al. (2010); *Habit* from Verplanken & Orbell (2003); *Personalization* from Xu et al. (2011); *Knowledge* from Xu et al. (2011); *Privacy Risk of Perception* from Diev & Hart (2004); *Privacy Intrusive Experience* from Xu et al. (2011a) and Li et al. (2016); *Privacy Policy* from Chang et al.

(2018), Xu et al. (2011) and *Intent to Disclose Personal Information* from Koehorst (2013).

The collected data was analyzed by SEM to evaluate the relationship between and among the different factors. In this method, many steps were conducted, such as Cronbach's Alpha, EFA, CFA, and finally, Structural Equation Modeling (SEM).

4. Research results

4.1. Sample description

After conducting the survey, out of 428 responses, 400 were selected to study. Among 400 valid answers, there are 147 men (36.8%), 252 women (63%) and 1 'other' responder (0.2%). There are 116 people aged 15-19 (29%). There are 128 people aged 20-24 (32%) and 156 people aged 25-29 (39%). All respondents used both social networks Facebook and Instagram, and 46.3% are long-time users with an average daily usage time of up to three hours.

4.2. Scale evaluation

Using Cronbach's Alpha coefficient to check the reliability of the scale with the standard for the study to be 0.7 and the correlation coefficient of the sum of the observed variables to be at least 0.3 (Nunally & Burstein, 1994), after the calculation and testing, for the nine variables: TRUST, PE, KNL, PREX, PEB, POLICY, PREX, PPR, DPI, only 2 variables PREX1 and PREX4 are bad variables and need to be removed.

4.3. Exploratory factor analysis (EFA)

The scales are then analyzed using factor analysis EFA after being tested using Cronbach's Alpha reliability coefficient. The principal components extraction method with Varimax rotation is applied. Hoang & Chu (2008) state that the extracted factors are the least. For this study, factor discovery analysis has been done concurrently with the variables. Independent, dependent, and intermediate variables were analyzed separately.

Exploratory factor analysis with independent variables

After checking the PREX1 and PREX2 variable type scales and conducting factor discovery analysis, in the process of running data, the type of variable TRUST5 and KNL6 (Running data for the second time) gives the result: KMO coefficient is 0.876 > 0.5. Exploratory factor analysis is consistent with the model, and Bartlett's test has a p-value equal to .000 < 0.05, extracted variance is 64.054%, greater than 50%, so the observed variable formed seven factors that explained 64.162% of the variation of the total variable and had an eigenvalue of 1.195 greater than 1.

Exploratory factor analysis of DPI (Dependent variable) and PPR (Intermediate variable)

Exploratory factor analysis was conducted for the DPI dependent variable and the PPR intermediate variable. In the process of running the data, a bad variable appeared and was removed. The running of the data included variables in the order of PPR9 (Running data for the second time) and DPI6, DPI7, PPR10 (Running data for the third time). The result was: KMO coefficient is 0.864 and Bartlett test has p-value of 0.000 < 0.05, extracted variance is 50.148% larger 50%, the eigenvalue is 2,413 which is greater than 1.

4.4. Confirmatory factor analysis (CFA)

After completing the exploratory factor analysis step, the confirmatory factor analysis step forms the basis for SEM and gives the final result.

During the CFA run, it was found that some indicators failed, so it was necessary to connect the two-way Covariance arrows to connect the pairs with high MI correction. The results were as follows: CMIN/DF index is 1,818 (CMIN/DF < 2); GFI index is 0.859 (0.8 < GFI < 0.9); CFI index is 0.912 (CFI > 0.9); LI is 0.902 (TLI > 0.9); RMSEA index is 0.045 (RMSEA < 0.8).

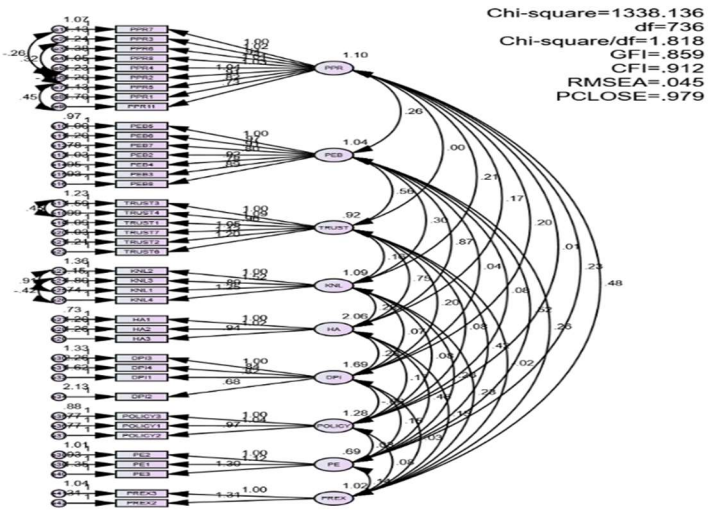

Figure 2: CFA Result
Source: Research data analysis.

Table 1: Summary of the normalized data

	Regression weights		Standardized regression weights		Regression weights		Standardized regression weights
	Estimate	**P (sig)**	**Estimate**		**Estimate**	**P (sig)**	**Estimate**
PPR<-TRUST	-.156	.020	-.161	DPI<-PPR	.187	.025	.143
PPR<-KNL	.039	.357	.052	DPI<-PEB	-.150	.162	-.118
PPR<-PE	.330	.000	.278	DPI<-HA	.200	.008	.221
PPR<-PREX	.401	.000	.400	DPI<-POLICY	-.068	.354	-.059

Source: Research data analysis.

4.5. Structural Equation Modeling (SEM)

When using the standard confidence level of 95%, the variable TRUST has a negative effect on the intermediate variable PPR; variable KNL does not affect the intermediate variable PPR; PE and PREX have a positive impact on the intermediate variable PPR. Of the four variables affecting the dependent variable, there is an intermediate variable, PPR, and the independent variable HA has an impact on the dependent variable DPI. The two independent variables PEB and POLICY have no impact on the dependent variable.

Of the four variables considered, only the KNL variable has no indirect influence on the dependent variable through the intermediate variable PPR. The remaining variables TRUST, PE, PREX, all indirectly affect the dependent variable through the intermediate variable PPR.

According to the SEM analysis, H1, H2, H5, H6, H8 are rejected. H3, H4 and H7 are accepted. That means Habit (HA) and Personalization (PE) positively affect the Intention to disclose personal information (DPI). Privacy Invasion Experience (PREX) has an indirect impact on the DPI by the mediation of Perception of Privacy risk (PPR).

Table 2: Indirect and direct effects of variables

Termites impact	Direct		Intermediate		Termites impact S.ES	Direct		Intermediate	
	S.ES	Sig.	S.ES	Sig.		Sig.	Sig.	S.ES	Sig.
TRUST->PPR->DPI			-0.023	0.018	KNL->PPR->DPI			0.007	0.265
PEB->DPI	-0.018	0.162			POLICY->DPI	-0.059	0.354		
HA->DPI	0.221	0.008			PREX->PPR->DPI			0.057	0.26
PE->PPR->DPI			0.040	0.020	PPR->DPI	0.143	0.025		

Source: Research data analysis.

5. Discussion

Privacy risk perception (PPR) influences variables including user trust variables -TRUST, personalization -PE, user knowledge -KNL, and privacy-infringed experience - PREX. Only the user knowledge variable is not statistically significant for the study, implying that it has no effect on the perception of privacy risk in this case study.

There is statistical significance in this study for the remaining three variables, with the variable user's trust affecting the perceived privacy risk variable, with the standard regression value based on the results of SEM model analysis being [-0.161]. This figure indicates that if user trust or confidence is high in social networking sites such as Facebook and Instagram, the perception of user privacy risk is low. This result is beneficial for the research team to have a fresh look at consumer behavior. For businesses, it takes a long time to develop a product that will gain the trust of customers. They must ensure that their products are as risk-free as possible in order to maintain consumer trust because when consumers choose to trust, they always expect the product's risk to be as low as possible or zero.

With a standardized regression coefficient of [0.278], the personalization variable has an impact on the perceived privacy risk variable. This number is significant if users' personal information is collected for advertising purposes. When businesses' products and services are improved, the perception of privacy risks regarding personal information on Facebook and Instagram increases. This result indicates that users are very concerned about their personal information being used maliciously at their own risk.

The final variable that influences privacy risk perception is the experience of privacy invasion, which has a normalized regression coefficient of [0.400] and explains whether or not a person has ever experienced a privacy breach. The facts experienced in practice can have a strong impact on people's perception. Similar to a business if the product launch process leaves a bad impression on the actual user experience, then the product is considered to have failed in launching and advertising because it was thought to be bad.

Next, the variables influencing social network users' intention to disclose personal information -DPI. Direct variables include privacy risk perception -PPR; consumer usage habits -HA; awareness of the benefits provided by social networks -PEB; and the privacy policies of those social networks -POLICY. Among the aforementioned variables, there are two that are not statistically significant for the study.

There is statistical significance in this study for the other two variables. The perceived privacy risk variable based on the results of the

SEM model analysis affects the user's intention to disclose personal information. With a normalized regression value of [0.143], this number indicates that when users are fully aware of the risks and consequences of stolen privacy, their intentions to post information are reduced and their vigilance for future posts is increased. Youn (2005) discovered that "adolescents are less likely to provide personal information to a website when they perceive a more serious privacy risk."

Based on the results of the SEM model analysis, the impact on the variable of user intention to disclose personal information has a standardized regression value of [0.221] for the variable usage habits of customers. This means that if a person has a habit of regularly updating images and information on social networks like Facebook and Instagram, it will continue indefinitely. According to Beldad et al. (2011), the benefits of information disclosure are not the only reason people share information, but also the "taste" of the disclosure itself (p.226). The findings of Strater and Richter (2007), who discovered that some of their respondents were unsure why they shared information, support the possibility of a strong influence of usage habits. Others didn't hesitate to provide personal information when asked because they were accustomed to filling out forms.

Furthermore, because of the direct impact of the PPR variable, there are three variables that have an indirect influence on social network users' intention to disclose personal information: -DPI, which is the user's trust variable, -TRUST, personalization -PE, and privacy-invaded experiences -PREX.

With a standardized regression coefficient of [-0.023], the user trust variable has an indirect impact on the information disclosure intention variable. If the user's trust or trust is high for social networking sites Facebook and Instagram, their perceived privacy risk will be low, affecting their intention to continue sharing in the future. This finding provides the research team with a fresh perspective on consumer behavior. Businesses must ensure that their products pose the least amount of risk in order to maintain consumer trust. When consumers choose to use a product, they can say that they trust and believe that the product meets their needs and that they intend to use it again in the future. Because TRUST has a negative effect (-) on PPR and PPR has a positive effect (+) on the DPI variable, TRUST's effect on DPI has the sign (-).

With a standardized regression coefficient of [0.040] for the personalization variable, which has an indirect impact on the information disclosure intention variable, this number indicates that the collection of users' personal information for advertising purposes increases as the number of products and services offered by businesses increases, as does the perception of privacy risks regarding personal information on Facebook. This will have an impact on users' willingness to use social networking sites in the future. Because PE has a positive (+) effect on PPR and PPR has a positive (+) effect on the DPI variable, the effect of PE on DPI has a (+) sign.

With a standardized regression coefficient of [0.057], PREX has an indirect effect on the variable of intention to disclose information for those who have had their privacy violated. This number is significant in explaining the behavior of a person who has experienced a privacy violation, has a very high awareness of privacy risks in the future and is wary of shared information. This result is very meaningful for the person. It has a strong impact on people's perceptions, behaviors, and attitudes. Just like a business, if the product launch process leaves a bad impression in the process of using its users, they will not continue to choose and trust the product, and the company's brand will leave a negative impression in the eyes of consumers. Because PREX has a positive effect (+) on PPR and PPR has a positive effect (+) on the DPI variable, PREX's effect on DPI has a (+) sign.

Users will gain more knowledge and a better understanding of their own personal information as a result of the above results, increasing their vigilance. At the same time, it provides Facebook and Instagram security administrators

with an overview of the situation, allowing them to develop solutions that help protect customers' personal information while minimizing risk for user privacy. Furthermore, based on the survey results, we make recommendations to social networking site users and social network service providers to help them better understand the risks associated with sharing personal information.

6. Conclusion

The survey of factors influencing risk perception and intention to disclose personal information began with seven independent variables discovered by us after reading and researching related reports and has been thoroughly edited through the qualitative process. The initial goal of the research paper is to investigate the factors influencing privacy risk perception and personal information disclosure and examines the relationship of perceived privacy risk with the intention to disclose personal information on Facebook and Instagram, thereby proposing a solution for the study. Based on the above goal, the research gathered data on variables thought to affect privacy risk perception and personal information disclosure and analyzed the SEM model to show the new relationship of the variables together.

Privacy risk perception influencing variables include user trust variables -TRUST, personalization -PE, user knowledge -KNL, and privacy-infringed experience -PREX. Only the user knowledge variable is not statistically significant for the study, implying that it has no effect on the perception of privacy risk in this case study.

With a standardized regression coefficient, the personalization variable has an impact on the perceived privacy risk variable. This number is significant if users' personal information is collected for advertising purposes. When businesses' products and services are improved, the perception of privacy risks regarding personal information on Facebook and Instagram increases. This result indicates that users are very concerned about their personal information being used maliciously at their own risk.

7. Limitation and further research

The research method used in this study is a convenient sampling method, with a small sample size, so the research results will not be as profound and provide the desired results as a larger sampling method. The study only surveys seven factors that influence the perception of privacy risks and the intention to disclose personal information on social media.

Future research should focus on the effect of demographic factors on user perception and behavior, as well as learning more about other factors that influence user perception and behavior. A longitudinal survey is needed to investigate the effects of perceived control over personal information, subjective norms, and privacy computational models on information disclosure of a private message.

References

Ajzen, I. (1991). The Theory of Planned Behavior. *Organizational Behavior and Human Decision processes, 50*(2), 179-211.

Ajzen, I. (2002). Residual Effects of Past on Later Behavior: Habituation and Reasoned Action Perspectives. *Personality and Social Psychology Review, 6*(2), 107-122.

Bauer, R. A. (1960). Consumer behavior as risk taking. In Proceedings of the 43rd National Conference of the American Marketing Association, June 15, 16, 17, Chicago, Illinois, 1960. American Marketing Association.

Beldad, A. et al. (2011). A Comprehensive Theoretical Framework for Personal Information-related Behaviors on the Internet. *The Information Society*, *27*(4), 220-232.

Beldad, A., De Jong, M., & Steehouder, M. (2011). I Trust not Therefore It Must be Risky: Determinants of the Perceived Risks of Disclosing Personal Data for e-Government Transactions. *Computers in Human Behavior*, *27(*6), 2233-2242.

Beuker, S. (2016). Privacy Paradox: Factors Influencing Disclosure of Personal Information among German and Dutch SNS Users. Master's Thesis, University of Twente.

Boyd, D. (2008). Why Youth (Heart) Social Network Sites: The Role of Networked Publics in Teenage Social Life. *MacArthur Foundation Series on Digital Learning – Youth, Identity, and Digital Media Volume* (ed. David Buckingham). Cambridge, MA: MIT Press.

Boyd, D. M., & Ellison, N. B. (2007). Social Network Sites: Definition, History, and Scholarship. *Journal of Computer-mediated Communication*, *13*(1), 210-230.

Burton-Jones, A., & Hubona, G. S. (2006). The Mediation of External Variables in the Technology Acceptance Model. *Information & Management, 43*(6), 706-717.

Caldwell, C., & Clapham, S. E. (2003). Organizational Trustworthiness: An International Perspective. *Journal of Business Ethics*, *47*(4), 349-364.

Chang, Y. et al. (2018). The Role of Privacy Policy on Consumers' Perceived Privacy. *Government Information Quarterly, 35*(3), 445-459.

Chen, H., & Atkin, D. (2021). Understanding Third-person Perception about Internet Privacy Risks. *New Media & Society*, *23*(3), 419-437.

Christofides, E., Muise, A., & Desmarais, S. (2009). Information Disclosure and Control on Facebook: Are They Two Sides of the Same Coin or Two Different Processes? *Cyberpsychology & Behavior, 12*(3), 341-345.

Cropanzano, R., & Mitchell, M. S. (2005). Social Exchange Theory: An Interdisciplinary Review. *Journal of Management, 31*(6), 874-900.

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

Culnan, M. J., & Bies, R. J. (2003). Consumer Privacy: Balancing Economic and Justice Considerations. *Journal of Social Issues, 59*(2), 323-342.

De Bruijn, G. J. et al. (2008). Saturated fat Consumption and the Theory of Planned Behaviour: Exploring Additive and Interactive Effects of Habit Strength. *Appetite, 51*(2), 318-323.

Dinev, T., & Hart, P. (2006). An Extended Privacy Calculus Model for e-Commerce Transactions. *Information Systems Research, 17*(1), 61-80.

Doll, W. J. et al. (1994). A Confirmatory Factor Analysis of the End-user Computing Satisfaction Instrument. *MIS Quarterly*, 453-461.

Ellison, N. B. et al. (2007). The Benefits of Facebook "Friends:" Social Capital and College Students' Use of Online Social Network sites. *Journal of Computer-Mediated Communication, 12*(4), 1143-1168.

Homans, G. C. (1958). Social Behavior as Exchange. *American Journal of Sociology, 63*(6), 597-606.

Hui, K. L. et al. (2007). The Value of Privacy Assurance: An Exploratory Field Experiment. *Mis Quarterly*, 19-33.

Joinson, A. N. et al. (2010). Privacy, Trust, and Self-Disclosure
Online. *Human–Computer Interaction*, *25*(1), 1-24.

Kim, B., & Kim, D. (2020). Understanding the Key Antecedents of Users' Disclosing Behaviors on Social Networking Sites: The Privacy Paradox. *Sustainability, 12*(12), 5163.

Kobsa, A. (2007). Privacy-enhanced Personalization. *Communications of the ACM, 50*(8), 24-33.

Koehorst, R. H. (2013). Personal Information Disclosure on Online Social Networks: An Empirical Study on the Predictors of Adolescences' Disclosure of Personal Information on Facebook. Master's Thesis, University of Twente.

Krasnova, H. et al. (2009). "It Won't Happen to Me!": Self-disclosure in Online Social Networks. *Conference: Proceedings of the 15th Americas Conference on Information Systems, AMCIS 2009*, San Francisco, California, USA, August 6-9, 2009.

Krasnova, H. et al. (2010). Online Social Networks: Why We Disclose. *Journal of Information Technology, 25*(2), 109-125.

Kremers, S. P., & Brug, J. (2008). Habit Strength of Physical Activity and Sedentary Behavior among Children and Adolescents. *Pediatric Exercise Science, 20*(1).

Kroll, T., & Stieglitz, S. (2021). Digital Nudging and Privacy: Improving Decisions about Self-Disclosure in Social Networks. *Behaviour & Information Technology*, *40*(1), 1-19.

Lankton, N. K., McKnight, D. H., & Thatcher, J. B. (2012). The Moderating Effects of Privacy Restrictiveness and Experience on Trusting Beliefs and Habit: An Empirical Test of Intention to Continue Using a Social Networking Website. *IEEE Transactions on Engineering Management, 59*(4), 654-665.

Limayem, M., Hirt, S. G., & Cheung, C. M. (2007). How Habit Limits the Predictive Power of Intention: The Case of Information Systems Continuance. *MIS Quarterly,* 705-737.

Loiacono, E., Carey, D., Misch, A., Spencer, A., & Speranza, R. (2012). Personality Impacts on Self-Disclosure Behavior on Social Networking Sites. *AMCIS 2012 Proceedings*. 6.

Mayer, R. C., & Davis, J. H. (1999). The Effect of the Performance Appraisal System on Trust for Management: A Field Quasi-experiment. *Journal of Applied Psychology, 84*(1), 123.

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). The Impact of Initial Consumer Trust on Intentions to Transact with a Web Site: A Trust Building Model. *Journal of Strategic Information Systems, 11*(3-4), 297-323.

Michaelidou, N., & Micevski, M. (2019). Consumers' Ethical Perceptions of Social Media Analytics Practices: Risks, Benefits and Potential Outcomes. *Journal of Business Research, 104,* 576-586.

Norberg, P. A. et al. (2007). The Privacy Paradox: Personal Information Disclosure Intentions Versus Behaviors. *Journal of Consumer Affairs*, *41*(1), 100-126.

Nunes, C. et al. (2011). Social Support and Stressful Life Events in Portuguese Multi-Problem Families. *International Journal of Developmental and Educational Psychology, 5*(1), 497-505.

Office of the Assistant for Administration & Management. Secretary Privacy Impact Assessment - OPA - Social Media Services. <https://www.dol.gov/agencies/oasam/centers-offices/ocio/privacy/opa/social-media> Accessed 1.1.2022.

Polites, G. L., & Karahanna, E. (2012). Shackled to the Status Quo: The Inhibiting Effects of Incumbent System Habit, Switching Costs, and Inertia on New System Acceptance. MIS Quarterly, 21-42.

Population Pyramids of the World from 1950 to 2100. The Population of Vietnam 2019. <https://www.populationpyramid.net/viet-nam/2019/> Accessed 1.1.2022.

Punj, G. (2017). Consumer Intentions to Falsify Personal Information Online: Unethical or Justifiable? *Journal of Marketing Management, 33*(15-16), 1402-1412.

Saunders, K. M., & Zucker, B. (1999). Counteracting Identity Fraud in the Information Age: The Identity Theft and Assumption Deterrence Act. *International Review of Law, Computers & Technology, 13(*2), 183-192.

Staksrud, E., & Livingstone, S. (2009). Children and Online Risk: Powerless Victims or Resourceful Participants? *Information, Communication & Society, 12*(3), 364-387.

Van Slyke, C. et al. (2006). Concern for Information Privacy and Online Consumer Purchasing. *Journal of the Association for Information Systems*, *7*(6), 1.

Verplanken, B., & Orbell, S. (2003). Reflections on Past Behavior: A Self-Report Index of Habit Strength. *Journal of Applied Social Psychology, 33*(6), 1313-1330.

Xu, H. (2007). The Effects of Self-construal and Perceived Control on Privacy Concerns. *Proceedings of the International Conference on Information Systems, ICIS 2007.* Montreal, Quebec, Canada.

Xu, H. et al. (2011). Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances. *Journal of the Association for Information Systems, 12*(12), 1.

Xu, H. et al. (2011). The Personalization Privacy Paradox: An Exploratory Study of Decision-making Process for Location-Aware Marketing. *Decision support Systems, 51*(1), 42-52.

Xu, H., Dinev, T., Smith, H. J., & Hart, P. (2008). Examining the Formation of Individual's Privacy Concerns: Toward an Integrative View. *Proceedings of the International Conference on Information Systems, ICIS 2008.* Paris, France.

Youn, S. (2005). Teenagers' Perceptions of Online Privacy and Coping Behaviors: A Risk-benefit Appraisal Approach. *Journal of Broadcasting & Electronic Media, 49*(1), 86-110.

Zhang, R., & Fu, J. S. (2020). Privacy Management and Self-disclosure on Social Network Sites: The Moderating Effects of Stress and Gender. *Journal of Computer-Mediated Communication, 25*(3), 236-251.

Zhao, L. et al. (2012). Disclosure Intention of Location-related Information in Location-based Social Network Services. *International Journal of Electronic Commerce, 16*(4), 53-90.