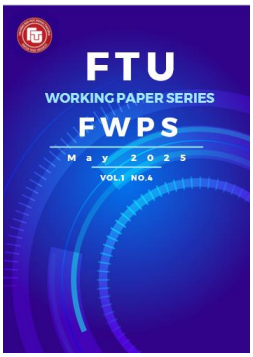


Working Paper 2025.1.4.16

- Vol. 1, No. 4

THE IMPACT OF PRIVACY AWARENESS ON E-TRUST: THE MEDIATING ROLE OF PRIVACY CONCERN

Nguyễn Bảo Minh Châu[1], Nguyễn Thanh Hường, Nguyễn Thu Hương, Đặng Thị Kim Anh

Sinh viên K61 CLC Quản trị kinh doanh quốc tế - Khoa Quản trị kinh doanh

Trường Đại học Ngoại thương, Hà Nội, Việt Nam

Đào Tâm Minh

Sinh viên K60 Tiếng Nhật thương mại – Khoa Tiếng Nhật

Trường Đại học Ngoại thương, Hà Nội, Việt Nam

Đỗ Hương Giang

Giảng viên Khoa Quản trị kinh doanh

Trường Đại học Ngoại thương, Hà Nội, Việt Nam

Abtract

The paper explores the relationship between privacy awareness and E-trust among Vietnamese online customers, specifically examining how privacy concerns mediate this relationship. The study was conducted in Vietnam through collecting data from 287 participants from January to February 2024. Analysis results from SMARTPLS 3 software show that privacy awareness has an indirect impact on E-trust through privacy concern. There is a difference in respondents' privacy awareness based on genders, majors (IT and non-IT). Thus, due to these valuable insights for increasing awareness about privacy among online users, the authors provide some recommendations for sellers and online platform providers.

[1] Tác giả liên hệ, Email: k61.2213250019@ftu.edu.vn

Keywords: Privacy awareness, privacy concern, E-trust, online customers, Vietnam

TÁC ĐỘNG CỦA NHẬN THỨC VỀ QUYỀN RIÊNG TƯ ĐỐI VỚI NIỀM TIN ĐIỆN TỬ (E-TRUST): VAI TRÒ TRUNG GIAN CỦA MỐI QUAN TÂM VỀ QUYỀN RIÊNG TƯ

Tóm tắt

Nghiên cứu tìm hiểu về mối quan hệ giữa nhận thức về quyền riêng tư và niềm tin điện tử (E-trust) của khách hàng trực tuyến tại Việt Nam, đồng thời xem xét vai trò trung gian của mối quan tâm đến quyền riêng tư trong quan hệ này. Nghiên cứu được thực hiện tại Việt Nam thông qua khảo sát 287 người từ tháng 1 đến tháng 2 năm 2024. Kết quả phân tích từ phần mềm SMARTPLS3 cho thấy nhận thức về quyền riêng tư có tác động gián tiếp đến niềm tin điện tử thông qua biến trung gian là mối quan tâm về quyền riêng tư. Ngoài ra, có sự khác biệt về nhận thức quyền riêng tư giữa các nhóm đối tượng theo giới tính và ngành học (công nghệ thông tin và chuyên ngành khác). Từ những phát hiện này, các tác giả đề xuất một số khuyến nghị cho người bán hàng và các nhà cung cấp nền tảng trực tuyến nhằm nâng cao nhận thức về quyền riêng tư của người dùng trực tuyến.

Từ khóa: Nhận thức về quyền riêng tư, mối quan tâm về quyền riêng tư, niềm tin điện tử, khách hàng trực tuyến, Việt Nam.

1. Introduction

The digital age thrives on a constant flow of personal data, fueling the convenience and personalization of online experiences. These personal data, which are exchanged and stored online, may be used for various purposes and by different parties. Individuals can conduct surveillance and collect data from one another (Krasnova et al., 2009). Studies by Acquisti et al. (2015) highlight a growing global awareness of online privacy issues, with individuals increasingly concerned about how their data is being used. In recent report, named "Corporate data responsibility: Bridging the trust chasm," which is based on two online surveys conducted by KPMG in April, May 2021, it indicated that 86% of the respondents said they feel a growing concern about data privacy, while 40% do not trust firms to use their data ethically in online platforms. Despite concerns about privacy, Tedeshci (2002) showed in his research study that 36% of internet buyers have no consideration for providing personal information to a new website as a trade for the possibility of receiving financial benefits. The concept of privacy has dramatically evolved with the trend of industrialization and automation. A newly raised provocation is people are getting accustomed to utilizing social media to disclose personal information, which raises awareness of privacy and security (Jeong & Kim, 2017).

The level of trust individuals place in online platforms is significantly influenced by their privacy concerns. Fukuyama (1996) showed trust is often vital in many economic operations that

can include unappreciated opportunistic behavior. Trust is also an issue, since sellers can easily take advantage of internet consumers (Jarvenpaa & Todd, 1996; Jarvenpaa & Tractinsky, 1999). Studies by Benbasat et al. (2008) underscore this point, highlighting trust as a key factor influencing user behavior in online environments – particularly when it comes to sensitive activities like online banking.

In Vietnam, Decree No. 52/2013/ND-CP is important in protecting customers' personal information when they participate in e-commerce activity. Our study aims to increase user's E-trust in terms of protecting privacy during accessing online platforms. This understanding will be pivotal in developing and implementing strategies that can both educate users about their privacy rights and build E-trust in online platforms. Ultimately, fostering a secure and trustworthy digital environment is essential for ensuring the continued growth and positive impact of the internet in Vietnam.

2. Theoretical framework and literature review

2.1. Theoretical framework

2.1.1. Privacy awareness

Deuker (2010) defined privacy awareness as the ability of individual users to perceive and evaluate the dangers involved in sharing personal information. Privacy awareness is "someone's ability to accurately perceive potential privacy threats. Phelps et al. (2000) defined privacy awareness as a person's understanding of privacy, including privacy policies, practices, and the use of shared data, as well as their awareness of the possible impact on their ability to preserve their privacy.

2.1.2. Privacy concern

Westin (1967) found that the definition of privacy is centered around the privacy concern. Privacy concern is defined as the people's perceptions of the dangers and potential negative effects of disclosed information (Cho et al., 2010; Zhou & Li, 2014). According to Zlatolas et al. (2015), privacy concerns indicate whether users are concerned about who will have access to the information they post on social networking services (SNSs). Nissenbaum (2004) introduced the concept of privacy as contextual integrity, suggesting that privacy concern may differ depending on the specific social contexts in which information is shared and accessed. This also coincides with the study of Dinev & Hart (2006), which investigated how internet privacy concerns may vary based on individuals' social awareness and intentions to engage in online transactions.

2.1.3. Trust and E-trust

According to Kim et al. (2005), trust in e-commerce is based on the consumer's faith in the processes. The idea that building trustworthy procedures is essential to an internet business's success

is supported by Grabosky (2001). In contrast, Taddeo (2009) characterizes e-trust as a type of trust that is exclusive to digital interactions in the absence of more conventional trust mechanisms like in-person contacts and tangible guarantees. According to Peštek et al. (2011), the primary factors influencing e-trust are quality, privacy, post-purchase care, and online accessibility.

2.1.4. Theory of Reasoned action (TRA)

Prior research on e-commerce has demonstrated that customers' intentions to do transactions online are a strong predictor of their actual involvement in online purchasing. These research works draw on the Theory of Reasoned Action - TRA (Fishbein & Ajzen, 1975) to investigate. The link between belief and intention is founded on the notion that individuals attempt to make logical judgments using the information available.

According to TRA, people's conduct is dictated by their desire to perform, which is influenced by two factors: their beliefs and their attitudes (beliefs → attitudes). The more confident a consumer is and the more likely they are to buy the goods, the higher their E-trust (Gefen et al., 2003).

Our model focuses on the first stage in what extent beliefs regarding the trustworthiness of website vendors, and e-commerce platforms. According to McCole et al. (2010), the relationship between E-trust in vendors and behavior towards online purchasing becomes more important when customers have higher privacy concerns. Another finding in this study is that the correlation between trust in the World Wide Web and a perspective towards buying goods online reduces when shoppers have greater security and privacy concerns.

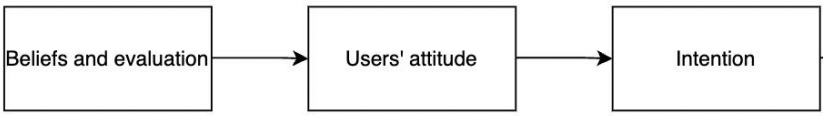


Figure 2.1.4. The concept of Theory of Reasoned Action (TRA)

Source: Fishbein & Ajzen (1975)

The TRA has been widely used to explain and predict various behaviors, such as health-related behaviors (Noar, 2004), consumer behaviors (Lim et al., 2016), and environmental behaviors (Yuriev et al., 2020).

2.1.5. Theory of Planned behavior (TPB)

According to the Theory of Planned activity (TPB), three factors—attitude, subjective norms, and perceived behavioral control—can affect a person's intention to engage in an activity. Intention is the closest predictor of actual action (Ajzen, 1991). Heirman et al. (2013) show that

people are more likely to do an activity they feel more confidence in than one they feel less skilled at. Yao & Linz (2008) and Saeri et al. (2014) have identified some empirical investigations that support the use of TPB to comprehend participation in online privacy protection behavior (PPB).

The TPB has also examined the relevant privacy concern, which people who have a high concern level are likely to curtail sharing information (Wirtz et al., 2007). Prior studies on the intentions to preserve online privacy indicated that while the subjective norm component was not significant, attitudes and perceived control were significantly positively and independently related with increased intentions to safeguard online privacy (Yao & Linz, 2008; Yousafzai et al., 2010)

Both TRA and TPB offer valuable insights into understanding how privacy awareness impacts trust through privacy concern. TRA emphasizes that individuals' behaviors are guided by their intentions, which are shaped by their beliefs and attitudes. In this context, privacy awareness influences individuals' beliefs about the risks associated with data handling and their attitudes toward the trustworthiness of online platforms. As individuals become more aware of privacy issues, their trust in these platforms is affected, since attitudes towards trust can significantly influence online behavior. Meanwhile, TPB builds on TRA by adding the concept of perceived behavioral control, suggesting that an individual's intention to engage in a behavior is influenced not only by attitudes but also by subjective norms and their sense of control.

When individuals are more aware of privacy concerns, their attitudes toward privacy protection and their perceived control over managing their personal information become more significant. Thus, by combining TRA and TPB, the model illustrates how privacy awareness shapes privacy concern, which subsequently influences trust, providing a comprehensive framework for understanding consumer behavior in digital environments.

2.2. Literature review

2.2.1. Privacy awareness and E-trust

E-Trust and Awareness among social media users have been studied. Koohang et al. (2021) state that knowledge is essential for safeguarding social media users from dangers and hazards. "An employee's overall knowledge and understanding of potential issues related to information security and their ramifications" is how Bulgurcu et al. (2010) describe information security awareness. Yerby et al. (2019) discovered that being aware of social media was crucial to protecting ourselves and preventing identity theft.

Consumer privacy awareness increases trust in one service provider, implying that customers' thoughts about having obtained adequate privacy awareness through a fair privacy statement raises their trust in the service provider (Sah & Jun, 2024). However, this study employs Privacy Calculus theory to examine customers' willingness to share personal information for Internet of Things (IoT) services, as well as the impact of procedural fairness in information disclosure. Thus our study proposes this hypothesis:

H1: Privacy awareness (PA) has positive impact on E-trust (TR)

2.2.2 Privacy awareness and privacy concern

The rise of the internet, social media, and information sharing has intensified privacy concerns. Researchers are investigating this area (George, 2004; Pavlou et al., 2007; Rose et al., 1999). Several factors influence privacy concerns, including how information is used, people's awareness of data collection, the sensitivity of the information, trust in the organization collecting it, and potential compensation for sharing data (Nowak & Phelps, 1992).

Privacy awareness has a positive impact on privacy concerns according to Warner & Wang (2019). There are 519 valid responses, using an exploratory factor analysis (EFA) to analyze the data for reliable results. Although most participants are aware of government surveillance, they suppose it will not be detrimental to them personally. The low usability of present privacy awareness systems contributes to a lack of understanding about the information acquired by social networking sites, their potential to cross-match data, and how it is used.

Therefore, the authors proposed this hypothesis:

H2: Privacy awareness (PA) has positive impact on privacy concern (PC)

2.2.3. Privacy concern and E-Trust

One of the most important concerns regarding online interaction is the risk of privacy breach. Various studies investigated the relationship between trust in online environments and privacy concerns which emphasize the detrimental effects of privacy concerns on user behavior (Kim, 2008; Hong & Thong, 2013). Dinev et al. (2013) examined how perceived risk mediates between privacy concern and trust in dark web browsing. They found that when users perceive their data vulnerable, their trust in online platforms declines. This highlights the importance of addressing data privacy and security concerns to foster trust online. Therefore, the authors proposed this hypothesis:

H3: Privacy concern (PC) has negative impact on E-trust (TR)

2.2.4. Privacy concern, privacy awareness and E-trust

Privacy awareness refers to an individual's understanding of privacy-related matters, including practices, policies, and the utilization of shared information. People who have a high level of privacy awareness are more likely to be concerned about privacy-related concerns, such as policies, procedures, and possible infractions (Dinev & Hart, 2005). According to Xu et al. (2008), people's attitude toward privacy values is positively impacted by their awareness of privacy issues in e-commerce.

Additionally, concerns about privacy might impede users' trust. When individuals harbor privacy concerns, they question whether companies gather excessive information and exploit it

without their consent. The act of self-disclosure can induce feelings of uncertainty and risk, resulting in reduced users' trust. As Alzaidi & Agag (2022), there is a negative correlation between privacy concerns and customer trust. Therefore, the authors proposed this hypothesis:

H4: Privacy concern has the mediating effect on the relationship between privacy awareness and E-trust

2.2.5. There are major and gender disparities in privacy awareness

McGill & Thompson (2018) found that gender differences in privacy perception were statistically significant. The result of this research stated that women exhibited considerably lower levels of both overall security behavior and perceived vulnerability compared to males. This is consistent with the need to investigate whether men and women in Vietnam have innately different levels of privacy awareness. Therefore, the authors proposed this hypothesis:

H5: There are differences in privacy awareness between genders

Raman & Pramod (2015) conducted a study of 1852 responses, examining user's awareness during online shopping. The study emphasizes the importance of raising privacy awareness by using Minitab 15 and SPSS was used to analyze the data. There are notable differences in the degree of privacy awareness between young adults in the 20–30 age range who graduated with degrees in Information Technology (IT) and those who did not. This study focused on users' perceptions and awareness of privacy when shopping online. This result supports the idea that studying Information Technology gives people a better awareness of user privacy settings, possible online risks, and data gathering methods. Therefore, the authors proposed this hypothesis:

H6: There are differences in privacy awareness between majors

2.2.6. Rresearch model

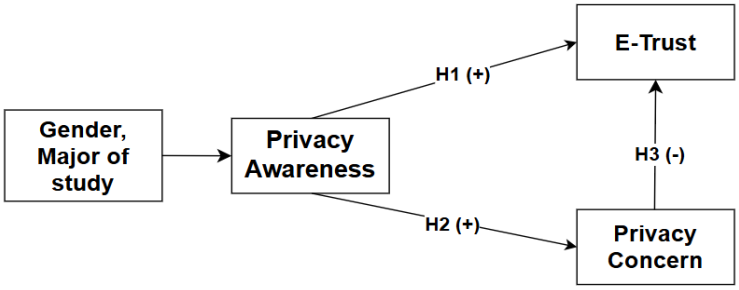


Figure 2.3.6. Research model

Source: The authors, 2024

3. Methodology

3.1. Measurement

To measure privacy awareness, four items are obtained from Xu *et al.* (2008). Six items assessing privacy concern are adapted from the scale developed by Xu et al. (2008), Wu *et al.* (2012). Four items regarding trust are adopted from the studies of Dwyer *et al.* (2007) and Krasnova *et al.* (2010)

3.2. Data collection

The author employs the convenience sampling (non-probability sampling) method as a data collecting method. Data was collected for a duration of one month, from January to February 2024 through Google Form. The survey was distributed to Vietnamese customers who had previously made online purchases.

According to Tabachnick & Fidell (2013), the sample size must adhere to the formula:

n >= 8m + 50

(n is the sample size, m is the number of independent variables in the model). This study involves 1 independent variables, so the minimum required size is calculated as 8*1 + 50 = 58. Out of 310 individuals surveyed, there are 287 satisfactory responses, constituting 92.6% of the total responses. Most of the respondents are in the 12-27 age group, which accounted for 88.2%. Among the respondents, 190 are female which comprises 66.2%. The number of IT respondents accounts for 20.2%.

3.3. Data processing method

The dataset will undergo a cleaning process utilizing Google Sheets, Excel, and will analyze descriptive statistics, Partial least squares structural equation modeling (PLS SEM), T-test, and ANOVA by SMARTPLS 3 and IBM SPSS 29.

4. Results

4.1. Demographic

The data used in this study was collected from 287 valid responses from Vietnamese people in terms of gender, age, and major.

Table 1. Demographic statistic of respondents

Criteria	Category	Percent
Gender	Female	66.2
	Male	31.0
	Other	2.8
Age	12 - 27	88.2
	28 - 43	7.3
	44 - 59	3.5
	>60	1.0
Major	IT	20.2
	Other	79.8

Source: Authors' own creation, 2024.

The survey revealed that 66.2% of respondents identified as female, 31% as male, and 2.8% identified as another gender. In terms of age, the majority (88.2%) were between 12 and 27 years old, while smaller groups represented other age ranges: 7.3% were aged 28–43, 3.5% were aged 44–59, and 1% were over 60. As for academic majors, 20.2% of participants were studying IT-related fields, while the remaining 79.8% were pursuing other disciplines.

4.2. Indicator reliability assessment

According to Hair et al. (2019), outer loading is used to assess the quality of observed variables. The authors excluded the observed variables PA4 because the outer loading was 0.629 which was less than 0.7.

4.3. Measurement model analysis

Table 2. The Reliability Test

Items	Factor Loadings	Cronbach's Alpha	Rho_A	CR	AVE
Privacy awareness (PA)					
PA1	0.063	0.77	0.786	0.865	0.681
PA2	0.848				
PA3	0.802				
Privacy concern (PC)					
PC1	0.845	0.892	0.898	0.918	0.652
PC2	0.857				
PC3	0.850				
PC4	0.785				
PC5	0.735				
PC6	0.762				
E-Trust (TR)					
TR1	0.814	0.822	0.827	0.882	0.652
TR2	0.845				
TR3	0.785				
TR4	0.783				

Source: Authors' own creation, 2024.

Author used the Cronbach's alpha test to assess the reliability of observed variables in scales, which helps to refine the research model and hypotheses. According to table 2, the Cronbach's Alpha values of all variables are higher than 0.6 and the composite reliability values are over 0.7 which demonstrates that the scale is highly accepted reliability. Besides, the index of Average Variance Extracted (AVE) of 3 variables is greater than 0.5 which shows that the measurement model satisfies the conditions of reliability and achieves convergent validity (Hair et al., 2014).

The factor loading coefficient of the observed variables must be greater than 0.5, and the factor loading coefficients ought to be concurrently greater than the cross-loading coefficients (Henseler et al., 2015). According to table 2, the factor loading coefficients of the observed variables are more than 0.5 and greater than the cross-loading coefficients. As a result, the measurement model meets discriminant validity's requirement.

Table 3. Fornell and Larcker criteria for discriminant validity testing

	PA	**PC**	**TR**
PA	**0.825**		
PC	0.392	**0.807**	
TR	0.211	-0.065	**0.807**

Source: Authors' own creation, 2024.

The discriminant validity assessment of a measurement model indicates the degree to which constructs are distinct and uncorrelated (Fornell & Larcker, 1981). As the result in table 3, the correlation coefficients in the same column are smaller than the square root values of AVE, which is in bold. Consequently, it may be said that AVE's square root values meet the requirement for discriminant validity.

Based on the results of analyzing the measurement model, it was found that all constructs in the research model achieved convergent and discriminant validity. From there, the authors can continue to conduct further analysis.

4.4. The structural model analysis

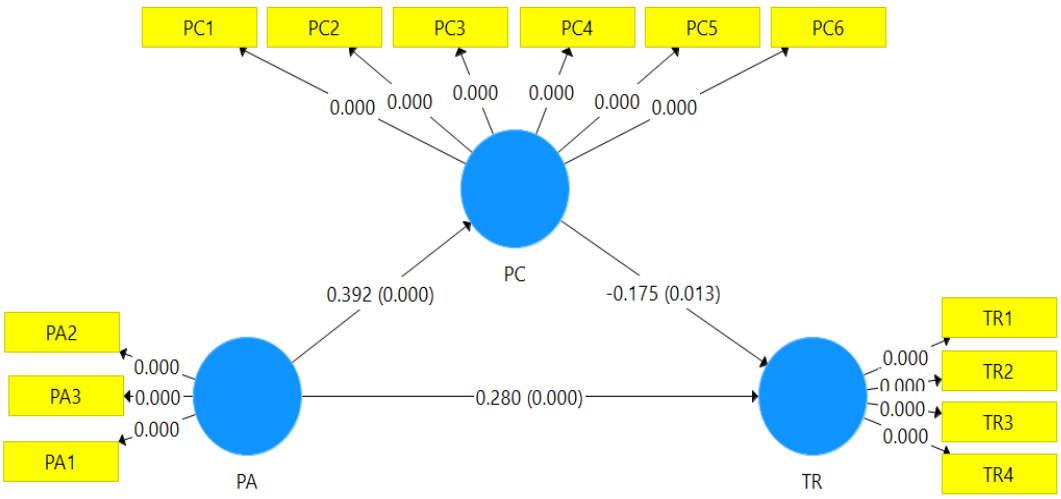
The VIF index was proposed by Hair et al. (2019) as a tool for assessing multicollinearity. Exogenous variables are shown in rows, and endogenous variables are shown in columns. All VIF indexes are lower than three, so there is no multicollinearity among the variables in the research model.

The author used the R-squared index to evaluate the explanatory power of the research model. The R-squared values for privacy concern (PC) and E-trust (TR) are 0.155 and 0.076 respectively. The predictive power is shown through the Q-squared index. Specifically, for variables privacy concern (PC) and E-trust (TR), this index stands at 0.096 and 0.041 respectively, indicating relatively low forecasting accuracy.

Table 4. PLS-SEM Analysis Results

Hypothesis	Relation	Impact	St. D	T values	P values	Results
H1	PA → TR	0.28	0.077	3.647	0.000	Accept
H2	PA → PC	0.392	0.058	6.702	0.000	Accept
H3	PC → TR	-0.175	0.071	2.477	0.013	Accept
H4	PA → PC → TR	-0.068	0.030	2.291	0.022	Accept

Source: Authors' own creation, 2024.



Source: The authors, 2024

The author group used the Bootstrapping approach (N = 1000) to test their hypothesis on direct effects. Table 4 presents the specific analysis results, which show that H1, H2, and H3 are all accepted at a 95% significance level. Furthermore, according to Cohen (2013), the f^2 index shows that PA has the greatest influence on PC. The remaining effects show relatively moderate impacts. Thus, it can be said that privacy awareness (PA) has a positive impact on buyer's E-trust

(TR) and privacy concern (PC) with the impacts of 0.392, 0.280 respectively, while the correlation between privacy concern (PC) and E-trust (TR) is negative at -0.175. The total effect of privacy awareness on trust is 0.211.

Regarding table 4, the results show that the independent variable (privacy awareness) has an indirect impact on the dependent variable (E-trust) with the impact of -0.068, and, there is a direct impact between privacy awareness and privacy concern (table 4). This means that when customers become more aware of privacy issues, they tend to be more concerned about them, making it more likely for them to lose E-trust while shopping online. Consequently, privacy concern plays a partial mediating role in the relationship between privacy awareness and E-trust.

4.4.1. Major

Table 5. Group statistics result of independent sample t-test

Major		N	Mean	Std. Deviation	Std. Error Mean	Leneve's test (sig)
PA	Non-IT	229	3.5830	0.74354	0.04913	0.007
	IT	58	3.8448	0.92697	0.12172	

Source: Authors' own creation, 2024.

The table 5 illustrates that there is a difference in respondents' privacy awareness based on majors, with the sig of the t-test equal to 0.05 and the Levene's test result being less than 0.05. Moreover, IT majors are more aware of privacy than non-IT majors; their respective means are 3.8448 and 3.5830. Therefore, hypothesis 4 is accepted.

4.4.2. Gender

Table 6. ANOVA test result of gender on privacy awareness

	N	Mean	F (sig)
Female	190	3.5697	0.021
Male	89	3.8118	
Other	8	3.2500	

Source: Authors' own creation, 2024.

Table 6 indicates that there is a difference in privacy awareness between people of various genders, with the sig value of the F test equal to 0.021 < 0.05. Furthermore, the mean level of privacy awareness among male respondents is greater (3.8118) than that of the female respondents and the "other" category (3.5697 and 3.2500, respectively). Consequently, hypothesis 5 is validated.

5. Discussion

The variable of privacy awareness has a positive influence on the level of customers' E-trust in online shopping. The result is aligned with several studies such as that of Liu et al. (2005), Hoadley et al. (2010), Sah & Jun (2024), which found the positive relationship between privacy awareness and E-trust of users upon virtual platforms. In fact, online shopping inherently involves sharing personal information. When online consumers are aware of their privacy and how their data is collected, stored, and used by online platforms, they will be less vulnerable. This increases the trustworthiness of online platforms, making users more eager to provide financial information and complete transactions.

Moreover, privacy awareness can act as a key factor in easing people's online decision (Kani-Zabihi & Helmhout, 2011). Table 4 shows a statistically significant positive correlation between privacy awareness and privacy concern. This result is consistent with the finding of Warner & Wang, (2019). Paramatar et al. (2018) also found that the more people are aware of the importance of safeguarding personal information, the higher they perceive privacy concern.

In addition, there is a significant negative correlation between privacy concern and E-trust which means that The higher the buyer's concern, the lower their trust is. This finding is also aligned with the result of Zorotheos & Kafeza (2009). These authors found that the reason why this users' has a negative impact on their E-trust is due to a lack of sufficient protection of personal information by the web site. In developing countries like Vietnam, the use of social media or various e-commerce platforms to shop online is still in the very first developmental stage. Therefore, sellers or retailers should help their customers to raise their E-trust about the privacy policies and securities of those platforms.

6. Conclusion and limitations

This research examined the interconnected web of privacy awareness, privacy concern, and E-trust within the Vietnamese online context. Our findings emphasize the positive impact of privacy awareness on privacy concerns. As individuals become more aware of the extent to which their data is collected and used, they naturally develop apprehensions and anxieties about potential misuse. PWC (2021) also stated that data security is an important factor contributing to building

E-trust with consumers: 59% of respondents indicated that they have become more concerned about protecting their personal data in the past six months. The result of that survey also stated that data security has a greater impact on building E-trust than other factors.

The Vietnamese government is taking steps to address these concerns and build a more secure digital environment. The 2018 Law on Personal Data Protection (PDPA) represents a significant effort to regulate data collection and use practices. Collaborative efforts between government agencies, technology platforms, and civil society organizations will be essential in fostering a culture of data privacy awareness and building E-trust in the Vietnamese digital landscape.

This research provides valuable insights and recommendations for three key objects in the Vietnamese online market: Vietnamese online customers, online sellers, and e-commerce platforms. Additionally, organizations like the Electronic Frontier Foundation (EFF), which offer educational materials and legal support on online privacy issues, can serve as models for empowering Vietnamese online shoppers by promoting privacy awareness.

For online shoppers, prioritizing privacy is key. They should choose reputable platforms like Lazada, Shopee, or Tiktok, research platform backgrounds, and limit the personal data they share. Using strong passwords, enabling two-factor authentication (2FA), and being aware of local consumer protection laws, such as Decree 13/2023/ND-CP, can help safeguard their information.

Online sellers in Vietnam must prioritize privacy and security to build E-trust and loyalty among customers. This starts with registering e-commerce ventures with authorities to ensure transparency and reduce fraud. Choosing secure e-commerce platforms and logistics partners is crucial. Sellers should also implement staff privacy training and a Code of Conduct focused on data confidentiality to enhance credibility and customer loyalty.

E-commerce platforms should prioritize security by implementing data encryption, secure payment methods, and transparent privacy policies. They can also integrate privacy-focused UI/UX elements to empower users. Exploring blockchain technology could offer future security enhancements, though challenges remain in infrastructure and regulation.

However, it is important to acknowledge the limitations of this study. Our research focused primarily on user perceptions and behaviors, relying on survey data and potentially missing out on the perspectives of platform developers and regulators. Additionally, the Vietnamese context is constantly evolving, with legal frameworks and user attitudes adapting to the digital landscape. Future research could address these limitations by incorporating a multi-stakeholder approach, including interviews with platform representatives and policymakers. Longitudinal studies tracking user perceptions over time could also provide valuable insights into how the interplay between privacy awareness, privacy concern, and E-trust unfolds within the dynamic Vietnamese digital environment.

Reference

Acquisti, A., Brandimarte, L. & Loewenstein, G. (2015). "Privacy and human behavior in the age of information." *Science*, Vol. 347 No. 6221, pp. 509–514.

Ajzen, I. (1991). "The Theory of planned behavior." *Organizational Behavior and Human Decision Processes*.

Alzaidi, M. S. & Agag, G. (2022). "The role of trust and privacy concerns in using social media for e-retail services: The moderating role of COVID-19." *Journal of Retailing and Consumer Services*, Vol. 68, pp. 103042.

Benbasat, I., Gefen, D. & Pavlou, P. A. (2008). "Trust in online environments." *Journal of Management Information Systems*, Vol. 24 No. 4, pp. 5–11.

Bulgurcu, B., Cavusoglu, H. & Benbasat, I. (2010). "Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness." *MIS Quarterly*, Vol. 34 No. 3, pp. 523–548.

Cho, H., Lee, J.-S. & Chung, S. (2010). "Optimistic bias about online privacy risks: Testing the moderating effects of perceived controllability and prior experience." *Computers in Human Behavior*, Vol. 26 No. 5, pp. 987–995.

Cohen, J. (2013). *Statistical power analysis for the behavioral sciences*. *Routledge*.

Deuker, A. (2010). "Addressing the privacy paradox by expanded privacy awareness – The example of context-aware services." *Privacy and Identity Management for Life: 5th IFIP WG 9.2, 9.6/11.4, 11.6, 11.7/PrimeLife International Summer School, Nice, France, September 7–11, 2009, Revised Selected Papers*, Vol. 5, pp. 275–283. *Springer Berlin Heidelberg*.

Dinev, T. & Hart, P. (2005). "Internet privacy concerns and social awareness as determinants of intention to transact." *International Journal of Electronic Commerce*, Vol. 10 No. 2, pp. 7–29.

Dinev, T. & Hart, P. (2006). "An extended privacy calculus model for e-commerce transactions." *Information Systems Research*, Vol. 17 No. 1, pp. 61–80.

Dinev, T., Xu, H., Smith, J. H. & Hart, P. (2013). "Information privacy and correlates: An empirical attempt to bridge and distinguish privacy-related concepts." *European Journal of Information Systems*, Vol. 22 No. 3, pp. 295–316.

Dwyer, C., Hiltz, S. & Passerini, K. (2007). "Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace." *AMCIS 2007 Proceedings*, pp. 339.

Fishbein, M. & Ajzen, I. (1975). *Belief, attitude, intention, and behavior: An introduction to theory and research*.

Fornell, C. & Larcker, D. F. (1981). "Evaluating structural equation models with unobservable variables and measurement error." *Journal of Marketing Research*, Vol. 18 No. 1, pp. 39–50.

Fukuyama, F. (1996). *Trust: The social virtues and the creation of prosperity*. Simon & Schuster.

Gambetta, D. (2000). "Can we trust trust." *Trust: Making and Breaking Cooperative Relation*, Electronic edition.

George, J. F. (2004). "The theory of planned behavior and Internet purchasing." *Internet Research*, Vol. 14 No. 3, pp. 198–212.

Gefen, D. & Straub, D. (2003). "Managing user trust in B2C e-services." *e-Service*, Vol. 2 No. 2, pp. 7–24.

Grabosky, P. (2001). "The nature of trust online." *The Age*, Vol. 23 No. 1, pp. 1–12.

Hair Jr, J. F., Sarstedt, M., Hopkins, L. & Kuppelwieser, V. G. (2014). "Partial least squares structural equation modeling (PLS-SEM): An emerging tool in business research." *European Business Review*, Vol. 26 No. 2, pp. 106–121.

Hair, J. F., Risher, J. J., Sarstedt, M. & Ringle, C. M. (2019). "When to use and how to report the results of PLS-SEM." *European Business Review*, Vol. 31 No. 1, pp. 2–24.

Heirman, W., Walrave, M. & Ponnet, K. (2013). "Predicting adolescents' disclosure of personal information in exchange for commercial incentives: An application of an extended theory of planned behavior." *Cyberpsychology, Behavior, and Social Networking*, Vol. 16 No. 2, pp. 81–87.

Henseler, J., Ringle, C. M. & Sarstedt, M. (2015). "A new criterion for assessing discriminant validity in variance-based structural equation modeling." *Journal of the Academy of Marketing Science*, Vol. 43, pp. 115–135.

Hoadley, C. M., Xu, H., Lee, J. J. & Rosson, M. B. (2010). "Privacy as information access and illusory control: The case of the Facebook News Feed privacy outcry." *Electronic Commerce Research and Applications*, Vol. 9 No. 1, pp. 50–60.

Hong, W. & Thong, J. Y. (2013). "The effects of electronic privacy information on user trust and risk perception in online environments." *Decision Support Systems*, Vol. 54 No. 3, pp. 1586–1597.

Jarvenpaa, S. L., Tractinsky, N. & Saarinen, L. (1999). "Consumer trust in an Internet store: A cross-cultural validation." *Journal of Computer-Mediated Communication*, Vol. 5 No. 2, pp. JCMC526.

Jeong, Y. & Kim, Y. (2017). "Privacy concerns on social networking sites: Interplay among posting types, content, and audiences." *Computers in Human Behavior*, Vol. 69, pp. 302–310.

Jarvenpaa, S. L. & Todd, P. A. (1996). "Consumer reactions to electronic shopping on the World Wide Web." *International Journal of Electronic Commerce*, Vol. 1 No. 2, pp. 59–88.

Kani-Zabihi, E. & Helmhout, M. (2011). "Increasing service users' privacy awareness by introducing on-line interactive privacy features." *Nordic Conference on Secure IT Systems*, Springer, pp. 131–148.

Kim, D. J., Ferrin, D. L. & Rao, H. R. (2008). "A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents." *Decision Support Systems*, Vol. 44 No. 2, pp. 544–564.

Kim, D. J., Song, Y. I., Braynov, S. B. & Rao, H. R. (2005). "A multidimensional trust formation model in B-to-C e-commerce: A conceptual framework and content analyses of academia/practitioner perspectives." *Decision Support Systems*, Vol. 40 No. 2, pp. 143–165.

Koohang, A., Floyd, K., Yerby, J. & Paliszkiewicz, J. (2021). "Social media privacy concerns, security concerns, trust, and awareness: Empirical validation of an instrument." *Issues in Information Systems*, Vol. 22 No. 2, pp. 133–145.

Krasnova, H., Günther, O., Spiekermann, S. & Koroleva, K. (2009). "Privacy concerns and identity in online social networks." *Identity in the Information Society*, Vol. 2, pp. 39–63.

Krasnova, H., Spiekermann, S., Koroleva, K. & Hildebrand, T. (2010). "Online social networks: Why we disclose." *Journal of Information Technology*, Vol. 25 No. 2, pp. 109–125.

KPMG (2023). *Corporate data responsibility: Bridging the consumer trust gap*. [online] Available at: https://kpmg.com/us/en/articles/2023/bridging-the-trust-chasm.html.

Lim, Y. J., Osman, A., Salahuddin, S. N., Romle, A. R. & Abdullah, S. (2016). "Factors influencing online shopping behavior: The mediating role of purchase intention." *Procedia Economics and Finance*, Vol. 35, pp. 401–410.

Liu, C., Marchewka, J. T., Lu, J. & Yu, C.-S. (2005). "Beyond concern—a privacy-trust-behavioral intention model of electronic commerce." *Information & Management*, Vol. 42 No. 2, pp. 289–304.

McCole, P., Ramsey, E. & Williams, J. (2010). "Trust considerations on attitudes towards online purchasing: The moderating effect of privacy and security concerns". *Journal of Business Research*, Vol. 63 No. 9–10, pp. 1018–1024.

McGill, T. & Thompson, N. (2018). "Gender differences in information security perceptions and behaviour". *29th Australasian Conference on Information Systems*.

McWhirter, D. A. (1992). *Privacy as a Constitutional Right: Sex, drugs and the Right to Life*. New York: Quorum Books.

Nissenbaum, H. (2004). "Privacy as contextual integrity". *Washington Law Review*, Vol. 79, pp. 119–157.

Noar, S. M. (2004). "A health educator's guide to theories of health behavior". *International Quarterly of Community Health Education*, Vol. 24 No. 1, pp. 75–92.

Nowak, G. J. & Phelps, J. E. (1992). "Understanding privacy concerns: An assessment of consumers' information-related knowledge and beliefs". *Journal of Direct Marketing*, Vol. 6 No. 4, pp. 28–39.

Paramarta, V., Jihad, M., Dharma, A., Hapsari, I. C., Sandhyaduhita, P. I. & Hidayanto, A. N. (2018). "Impact of user awareness, trust, and privacy concerns on sharing personal information on social media: Facebook, Twitter, and Instagram". *2018 International Conference on Advanced Computer Science and Information Systems (ICACSIS)*, pp. 271–276.

Pavlou, P. A., Liang, H. & Xue, Y. (2007). "Understanding and mitigating uncertainty in online exchange relationships: A principal-agent perspective". *MIS Quarterly*, Vol. 31 No. 1, pp. 105–136.

Peštek, A., Resić, E. & Nožica, M. (2011). "Model of trust in e-transactions". *Economic Research–Ekonomska Istraživanja*, Vol. 24 No. 3, pp. 131–146.

Phelps, J., Nowak, G. & Ferrell, E. (2000). "Privacy concerns and consumer willingness to provide personal information". *Journal of Public Policy & Marketing*, Vol. 19 No. 1, pp. 27–41.

PWC (2021). "A time for hope: Consumers' outlook brightens despite headwinds. Highlights from PwC's December 2021 Global Consumer Insights Pulse Survey. Vaccination status and flexible workstyle influence consumer optimism". *PwC Global Consumer Markets Insights*. Available at: https://www.pwc.com/gx/en/consumer-markets/consumer-insights-survey/november-2021/gcis-placemate-december-2021.pdf

Raman, R. & Pramod, D. (2015). "A study on user perception and awareness related to online privacy during online shopping". *Journal of Theoretical & Applied Information Technology*, Vol. 77 No. 3.

Rose, G., Khoo, H. M. & Straub, D. (1999). "Current technological impediments to business-to-consumer electronic commerce". *Communications of the Association for Information Systems*, Vol. 1 No. 1, pp. 16.

Saeri, A. K., Ogilvie, C., La Macchia, S. T., Smith, J. R. & Louis, W. R. (2014). "Predicting Facebook users' online privacy protection: Risk, trust, norm focus theory, and the theory of planned behavior". *The Journal of Social Psychology*, Vol. 154 No. 4, pp. 352–369.

Sah, J. & Jun, S. (2024). "The role of consumers' privacy awareness in the privacy calculus for IoT services". *International Journal of Human–Computer Interaction*, Vol. 40 No. 12, pp. 3173–3184.

Tabachnick, B. G., Fidell, L. S. & Ullman, J. B. (2013). *Using Multivariate Statistics*. Boston, MA: Pearson.

Taddeo, M. (2009). "Defining trust and e-trust: From old theories to new problems". *International Journal of Technology and Human Interaction (IJTHI)*, Vol. 5 No. 2, pp. 23–35.

Tedeschi, B. (2002). "Everybody talks about online privacy, but few do anything about it". *New York Times*, Vol. 3 No. 6.

Warner, M. & Wang, V. (2019) "Self-censorship in social networking sites (SNSs) – privacy concerns, privacy awareness, perceived vulnerability and information management", *Journal of Information, Communication and Ethics in Society*, Vol. 17 No. 4, pp. 375–394.

Westin, A. F. (1967) "Privacy and freedom Atheneum", *New York*, Vol. 7 No. 1967, pp. 431–453.

Williamson, O. E. (1985) *The Economic Institutions of Capitalism: Firms, Markets, Relational Contracting*. Free Press.

Wirtz, J., Lwin, M. O. & Williams, J. D. (2007) "Causes and consequences of consumer online privacy concern", *International Journal of Service Industry Management*, Vol. 18 No. 4, pp. 326–348.

Wu, K.-W., Huang, S. Y., Yen, D. C. & Popova, I. (2012) "The effect of online privacy policy on consumer privacy concern and trust", *Computers in Human Behavior*, Vol. 28 No. 3, pp. 889–897.

Xu, H., Dinev, T., Smith, H. J. & Hart, P. (2008) "Examining the formation of individual's privacy concerns: Toward an integrative view".

Yao, M. Z. & Linz, D. G. (2008) "Predicting self-protections of online privacy", *CyberPsychology & Behavior*, Vol. 11 No. 5, pp. 615–617.

Yerby, J., Koohang, A. & Paliszkiewicz, J. (2019) "Social media privacy concerns and risk beliefs", *Online Journal of Applied Knowledge Management*, Vol. 7 No. 1, pp. 1–13.

Yousafzai, S. Y., Foxall, G. R. & Pallister, J. G. (2010) "Explaining internet banking behavior: theory of reasoned action, theory of planned behavior, or technology acceptance model?", *Journal of Applied Social Psychology*, Vol. 40 No. 5, pp. 1172–1202.

Yuriev, A., Dahmen, M., Paillé, P., Boiral, O. & Guillaumie, L. (2020) “Pro-environmental behaviors through the lens of the theory of planned behavior: A scoping review”, *Resources, Conservation and Recycling*, Vol. 155, pp. 104660.

Zhou, T. & Li, H. (2014) “Understanding mobile SNS continuance usage in China from the perspectives of social influence and privacy concern”, *Computers in Human Behavior*, Vol. 37, pp. 283–289.

Zorotheos, A. & Kafeza, E. (2009) “Users' perceptions on privacy and their intention to transact online: a study on Greek internet users”, *Direct Marketing: An International Journal*, Vol. 3 No. 2, pp. 139–153.

Zlatolas, L. N., Welzer, T., Heričko, M. & Hölbl, M. (2015) “Privacy antecedents for SNS self-disclosure: The case of Facebook”, *Computers in Human Behavior*, Vol. 45, pp. 158–167.