ISSN 2409-2665
Journal of Logistics, Informatics and Service Science
Vol. 9 (2022) No.3, pp.31-44
DOI:10.33168/LISS.2022.0303

The Influence of Individuals' Concerns about Organization's Privacy Information Practices on Customers' Online Purchase Intentions: The Mediating Role of Online Trust

Bui Thanh Khoa [1+], Tran Trong Huynh [2]

[1] Industrial University of Ho Chi Minh City, Vietnam
[2] FPT University, Ha Noi, Vietnam

[+]*buithanhkhoa@iuh.edu.vn (Corresponding author), huynhtt4@fe.edu.vn*

Abstract. In daily online transactions, customers may disclose personal information that others may use to invade privacy, such as sensitive information such as IP address, email address, current physical location, and home or work address. Worrying about compromised privacy can lead to negative behaviors such as stopping transactions on an e-commerce site. Therefore, the objective of this study was to analyze the influence of individuals' concerns about an organization's privacy information practices (ICOPIP) on customers' online purchase intentions, in which online trust is considered a mediating variable. The study adopted an online questionnaire surveying 467 respondents aged 18 and over. Research results show that ICOPIP positively impacts consumers' trust and purchase intention. In addition, trust is a partial mediator in the relationship between ICIPIP and purchase intention. The research results also contribute to some managerial implications for online businesses.

Keywords: privacy information practices, online trust, purchase intention.

1. Introduction

Smartphones, mobile commerce, big data analytics, artificial intelligence (AI), and the Internet of Things (IoT) are all examples of how advancements in information and communication technology (ICT) have raised the bar for our day-to-day experiences. Advances in information technology hold great potential for businesses as the Internet becomes a practical and efficient way of delivering services electronically as health, education, and trade. While this may benefit providers and consumers, collecting greater personal data is risky. The top worry of online users is privacy owing to the sensitivity of personal information (Hong & Thong, 2013). Furthermore, a recent study of 25 countries found that more than half of respondents are more concerned about their online privacy than they were a year ago (Bricker et al., 2018). According to a recent poll, 85 percent of businesses believe their consumers have little control over how their personal information is utilized (Accenture, 2018). Indeed, Individuals' Concerns about Organization's Privacy Information Practices (ICOPIP) have grown dramatically due to the creation of a hyper-connected network and modern technology and extensively reported data breach cases (Conger et al., 2013). For instance, a data breach at Target revealed the debit and credit card details of millions of consumers. More than 100 million individuals may have stolen their identities due to the data breach at Equifax's consumer credit reporting agency. Without the knowledge or consent of 87 million users, Facebook sent their information to Cambridge Analytica in 2018. Concern over the potential disclosure of personally identifiable information is a common source of stress for individuals (Yun et al., 2019), which causes them to be hesitant to accept new technology or use internet services. As a result, businesses must gain a solid grasp of the nature and extent of ICOPIP in different settings.

ICOPIP may jeopardize their capacity to control personal information (H. J. Smith et al., 1996). ICOPIP is defined by Belanger et al. (2002) as an individual's desire to control data about oneself. In response to increased privacy concerns, academics have looked at various ICOPIP - related problems (Preibusch, 2013). However, researchers are often unaware of the study settings and conceptions that must be investigated to make meaningful additions to the literature. This is because researchers have varying interests and rely on a wide range of theories to investigate the phenomena that ICOPIP is concerned with and because study environments and constructs seem to evolve as technology advances. Because of this problem, efforts to further ICOPIP concern research may be fruitless. In light of the growing body of literature on ICOPIP topics, it is timely and important to reflect on the field's historical development by reviewing works from the past that have dealt with similar topics. Data like this would be invaluable to researchers in gauging the current state of the literature, pinpointing research gaps, and focusing their efforts on areas that have been overlooked or require more investigation.

Many studies are especially interested in investigating how ICOPIP research has changed regarding ICOPIP settings and research components. Researchers have recently recommended an investigation into the circumstances of ICOPIP (Mutimukwe et al., 2020; Yun et al., 2019; Zhang et al., 2018). In addition, it has been stated that ICOPIP research is not based on a consistent theoretical paradigm (Li, 2011), preventing academics from building a solid foundation for ICOPIP study. First, knowing what kinds of contexts and theoretical frameworks have been tested and how they have evolved is important. Trust and Purchase Intentions are two well-known constructs in business research. Based on the S-O-R theory (Stimulus–Organism–Response), trust can be seen as the buyer's perception of the privacy of buying online, and the final response is the buying behavior as purchase intention or loyalty. The stimulus was a personal concern about the organization's information security practices. Loss of agency in financial dealings and privacy raises issues (Dinev & Hart, 2003). If customers know that businesses have implemented policies to protect their private information, they will have confidence in the business (Dehghani Soltani et al., 2019; S. K. Lee & Min, 2021). The outcome of individual concerns about an organization's information security practices and trust is the intention to purchase goods on websites or e-commerce exchanges (Dehghani Soltani et al., 2019).

This study explores the relationship between individual concerns about the organization's privacy information practices, trust, and online purchase intention of customers on e-commerce sites in Vietnam. From there, the study will propose managerial implications for online businesses in Vietnam in order to improve the initial trust, as well as the online purchase intention of customers. In addition to the introduction, this study contains contents related to the theoretical basis and research methods. The research results will be the basis for discussing and proposing managerial implications for enterprises.

2. Literature review

2.1. Theoretical model

The SOR theory, presented by Mehrabian and Russell (1974), has gotten much attention in numerous research domains over the last several decades because of its intuitive and strong exploratory character in studying human behavior. According to the idea, Response behavior (R), like avoidance or approach, is affected by emotional Organism (O) and is preceded by environmental stimuli (S). Because of its broad application, the researchers adjusted the SOR technique in the unique study setting and integrated cognitive and emotional variables. The study's catalyst was personal worry about the organization's privacy information policies. Privacy concerns stem from a lack of control over transactions, particularly the flow of information. Customers will have more trust in a company if they know it has rules to secure their personal information. Individuals' intentions to acquire items on websites or via e-

commerce exchanges result from their worries about an organization's information security measures and trust. Figure 1 depicts the suggested research model.

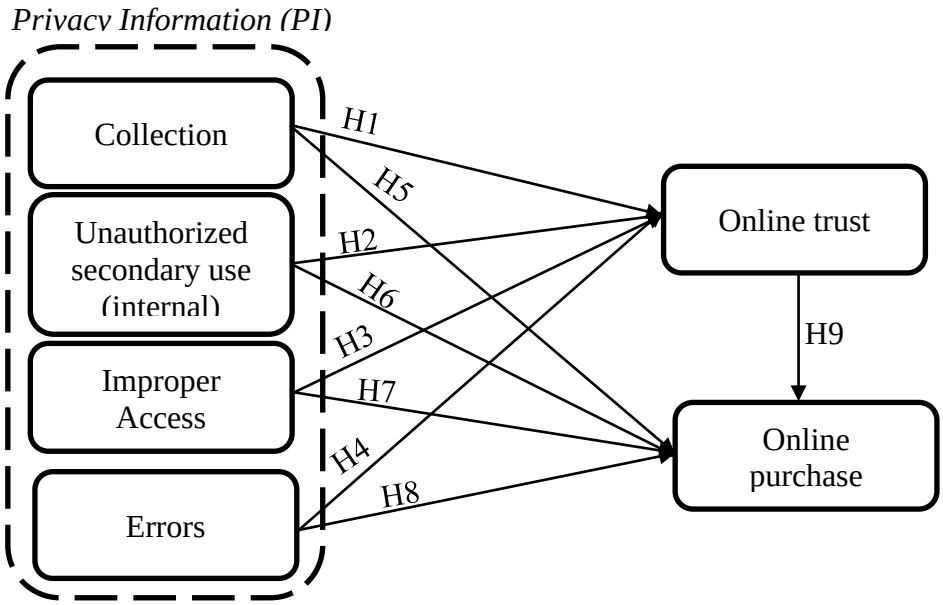

Fig. 1: Theoretical model.

2.2. Research hypotheses development

H. J. Smith et al. (1996) introduced the idea of ICOPIP. People's concerns about organizations' information privacy rules were divided into four basic categories. Among them include collection, Internal unauthorized secondary (internal), Improper access (external), and errors. The worry that vast amounts of personally identifiable information are being acquired and stored in databases is called a collection. Concern that information gathered from individuals for one purpose is used for another, secondary purpose (internally within the same company) without the people's consent. Improper access refers to the problem of information about persons being freely available to others who are not formally allowed to view or use this information. Finally, the error concerns inadequate personal data protection solutions against purposeful and inadvertent access.

Users' privacy concerns have grown in tandem with e-services as a delivery mechanism since technological advancements have made it easier for businesses to store, process, and profit from customers' personal information. This can lower people's confidence in their ability to manage their private data and increase their awareness of the risks associated with doing so (Featherman & Pavlou, 2003). Because bad user perceptions hurt service provider reputations and may impede

service delivery by reducing users' trust and willingness to give personal information, service providers must have a deep familiarity with customers' privacy issues.

The previous study has also indicated that customers are more inclined to trust organizations with their privacy information (PI) when they perceive they have control over their information (Chang et al., 2018; Taddei & Contena, 2013). A lack of perceived control will reduce customer trust in a corporation (Liu et al., 2005). As a consequence, this study proposed the hypotheses:

H1: Collection's PI perception impacts positively on the customer's online trust

H2: Unauthorized secondary use (internal) 's PI perception impacts positively on the customer's online trust

H3: Improper access's PI perception impacts positively on the customer's online trust

H4: Error's PI perception impacts positively on the customer's online trust

As stated by Stewart and Segars (2002), concerns about information privacy impact behavioral intentions. They contended that a person with high levels of CFIP would take proactive actions to decrease the probability of their privacy being violated, such as deleting oneself from mailing lists, avoiding submitting personal information online, and so on (Zhou, 2020). However, if customers know that the business has a privacy policy, customers can confidently purchase on the website. However, if customers know that the business has policies to protect their privacy, they can confidently purchase on the website (Frik & Mittone, 2019). Hence, the study proposes some hypotheses as follows:

H5: Collection's PI perception impacts positively on online purchase intention

H6: Unauthorized secondary use (internal) 's PI perception impacts positively on online purchase intention

H7: Improper access's PI perception impacts positively on online purchase intention

H8: Error's PI perception impacts positively on online purchase intention

Several studies have shown that trust influences purchasing intentions toward internet businesses favorably (Ha & Janda, 2014). Bock et al. (2012) demonstrated that consumers' levels of trust play a crucial role in determining whether they would use a website. Similarly, Dennis et al. (2010) argue that consumers' level of trust is a major factor in deciding whether or not they will make an online purchase. Ha and Janda (2014) revealed that consumers' trust in web-based e-commerce significantly impacted their propensity to make purchases. Consumers who have faith in a company are more likely to purchase on the website (J. Lee et al., 2011). A hypothesis is offered in light of these data, which is as follows:

H9: Customer online trust impacts positively on online purchase intention.

3. Research Method

This study applied the quantitative research method. All scales used to test the model's dependent and independent variables were 5-option Likert-type, with 1 meaning "completely disagree" and 5 meaning "completely agree." ICOPIP, including four factors as Collection (COL), Unauthorized secondary use (internal) (USU), Improper Access (IMA), and Error (ERR), were proposed by H. J. Smith *et al.* (1996); In addition, this study modified Valdez's user trust scale (OT) (Valdez, 2021), and online purchase intention (IB) scale are applied based on Zhu *et al.* (2020).

For data collection, questionnaires were delivered online to personnel from various occupations, ages, sex. For a variety of reasons, only 467 legitimate surveys were received. According to Table 1, 51.6 percent of respondents are males, and 48.4 percent are female. Regarding age, most people fall into the categories corresponding from 18 to 45 years old. The respondents are mostly office workers (25.1 percent), lecturers (20.1 percent), government employees (19.9%), and the rest include homemakers and students. The data collection method in this research was purposive sampling. At the beginning of the questionnaire will be screening questions such as "Have you ever made an online purchase?", "Have you been affected by improper use of personal information?" and "Do you care about your privacy?". This process will help filter the respondents and find the right respondents for the survey content.

Table 1. The respondent information.

		Frequency	Percent
Gender	Male	241	51.6
	Female	226	48.4
Age group	18 - 25	123	26.3
	26 - 35	120	25.7
	36 - 45	115	24.6
	> 45	109	23.3
Occupation	Housewife	81	17.3
	Student	82	17.6
	Office worker	117	25.1
	Lecturer	94	20.1
	Government employee	93	19.9

This study analyzed structural equation models based on variance using the partial least squares (PLS) method. The data was analyzed using smart-pls 3.7.

For data collection, questionnaires were delivered online to personnel from various occupation, age, sex. For a variety of reasons, only 467 legitimate surveys were received. According to Table 1, 51.6 percent of respondents are males, and 48.4 percent are female. Regarding age, most people fall into the categories corresponding from 18 to 45 years old. The respondents are mostly office workers (25.1 percent), lecturers (20.1 percent), government employees (19.9%), and the rest include homemakers and students. The data collection method in this research was purposive sampling. At the beginning of the questionnaire will be screening questions such as "Have you ever made an online purchase?", "Have you been affected by improper use of personal information?" and "Do you care about your privacy?". This process will help filter the respondents and find the right respondents for the survey content.

4. Results

This study followed the data analysis process proposed by Hair Jr et al. (2016). Firstly, the evaluation of measurement models was the first step, and the research would evaluate the structural model.

4.1. Measurement model assessment

The information shown in Table 2 is what is needed to begin verifying the measurement model by establishing the items' dependability. This investigation assessed all latent variables (reflective constructs) in mode A. All items' outer loadings (OL) and the COL, ERR, IMA, USU, OT, and IB exceeded the minimum threshold of 0.707 (Carmines & Zeller, 1979). Each of the constructs also had a Cronbach Alpha (CA) and Composite Reliability (CR) of more than 0.7. Also, the Average Variance Extracted (AVE) for the six components was larger than 0.5. In this sense, all notions have validity and reliability.

Table 2: The reliability and convergent validity.

Construct	CA	CR	AVE	OL
COL	0.862	0.907	0.709	[0.796 - 0.911]
ERR	0.877	0.916	0.731	[0.851 - 0.858]
IB	0.814	0.878	0.643	[0.763 - 0.834]
IMA	0.881	0.926	0.807	[0.890 - 0.913]
OT	0.903	0.932	0.775	[0.868 - 0.914]
USU	0.929	0.95	0.825	[0.894 - 0.935]

Fornell-Larcker criterion and Cohen's kappa statistic were used to evaluate the discriminant validity of the different constructs (latent variables). As shown in Table 3, the Fornell-Larcker criterion is strictly satisfied under all conditions. Diagonal components represent the square root of the variance between the constructs and their respective measures. The relationships between different constructions are the out-

of-the-diagonal components. Discriminant validity requires that diagonal elements be larger than off-diagonal ones.

Table 3: Discriminant validity.

Construct	COL	ERR	IB	IMA	OT	USU
COL	0.842					
ERR	0.374	0.855				
IB	0.639	0.619	0.802			
IMA	0.523	0.406	0.655	0.898		
OT	0.452	0.473	0.642	0.53	0.88	
USU	0.438	0.442	0.693	0.469	0.496	0.908

4.2. Evaluation of structural model

The structural model's path coefficients, f^2 value, R^2 values, and Q^2 test were analyzed, along with their signs, sizes, and statistical significances. Bootstrapping with 5,000 replicates was used to get the t-statistics for the data, confidence intervals, and the significance of the associations, as advised by Hair Jr *et al.* (2016).

In Table 4, R^2_{IB} suggests 74.9% of IB's change from COL, ER, IMA, USU, and OT; hence, this is a good predictor for IB. Moreover, all effect sizes (f^2) were larger than 0.02; this result pointed out the relevance of COL, ERR, IMA, and USU with IB and OT, as well as the relationship between OT and IB. The Q^2 values are larger than zero, which emphasizes the model's predictive power. Finally, VIF values were less than 2, which means there are no collinearity issues in this model.

Table 4: f^2, R^2, Q^2, and VIF.

Construct	f^2		R^2	VIF		Q^2
	IB	*OT*		*IB*	*OT*	
COL	0.143	0.021		1.534	1.502	
ERR	0.152	0.06		1.434	1.353	
IB			0.749			0.471
IMA	0.1	0.079		1.703	1.577	
OT	0.061		0.414	1.707		0.315
USU	0.245	0.052		1.561	1.483	

To Table 5, because all direct impacts are significant and positive, the data validates all of the model's assumptions.

Table 5. Path coefficient and hypotheses result.

Relationship	β	Std. Deviation	t-value	Hypothesis	Result
COL -> OT	0.136	0.054	2.5	H1	Accepted
USU -> OT	0.213	0.059	3.614	H2	Accepted

Relationship	β	Std. Deviation	t-value	Hypothesis	Result
IMA -> OT	0.271	0.054	4.975	H3	Accepted
ERR -> OT	0.218	0.05	4.33	H4	Accepted
COL -> IB	0.235	0.041	5.708	H5	Accepted
USU -> IB	0.31	0.039	7.892	H6	Accepted
IMA -> IB	0.207	0.046	4.524	H7	Accepted
ERR -> IB	0.234	0.045	5.193	H8	Accepted
OT -> IB	0.161	0.041	3.971	H9	Accepted

4.3. Mediating role of online trust

In addition to the results in table 5, the significant relationship between four factors forming ICOIP and OT; and the relationship between OT and IB was confirmed. The research result in Table 6 also showed that through online trust, the influence of ICOPIP on online purchase intention is reduced although the relationship is still statistically significant, specifically as follows, $\beta_{COL->OT->IB} = 0.022$ (t-value = 0.035), $\beta_{ERR->OT->IB} = 0.035$ (t-value = 0.012), $\beta_{IMA->OT->IB} = 0.044$ (t-value = 0.006), $\beta_{USU->OT->IB} = 0.034$ (t-value = 0.003). Hence, online trust is the mediator in the relationship between ICOIP and IB.

Table 6: Specific indirect effects of ICOIP on IB.

	β	Standard Deviation	T- value
COL -> OT -> IB	0.022	0.01	2.104
ERR -> OT -> IB	0.035	0.014	2.518
IMA -> OT -> IB	0.044	0.016	2.746
USU -> OT -> IB	0.034	0.012	2.965

5. Discussion

According to Solove (2007), business information practices (or inadequate organizational privacy policies) may lead to a wide range of privacy difficulties relating to customers' worries about the confidentiality of their personal information, providing the foundation for a more nuanced understanding of the concept of privacy. However, consumer studies concentrating on individual behaviors are overwhelmingly prevalent in the privacy literature, whereas research on information practices from an organizational viewpoint is mostly absent (Smith *et al.*, 2011). The data collecting and transmission process have various blind spots, including whether people may exert meaningful control over their information in all settings. The inference is that privacy management is not merely an issue of human behavior, but rather an integral part of institutional framework, as seen by prevalent trends in the business and nonprofit sectors. Strong correlations were shown between ICOPIP, online trust, and e-commerce buyers' propensity to make a transaction.

Firstly, this result pointed out that four dimensions of ICOPIP have positive impact on online trust; in particularly, (1) collection (β = 0.136, t-value = 2.5), (2) Unauthorized secondary use (internal) (β = 0.213, t-value = 3.614), (3) Improper Access (β = 0.271, t-value = 4.975), (4) Error (β = 0.218, t-value = 4.33). Therefore, hypothesis H1 was accepted in 95% of the confidence level; H2, H3, and H4 were supported at the confidence level of 99%. The Error and Improper access's privacy information perception has a stronger impact on online trust than the rest. In many cases, customers will have many trusts if they understand that the enterprise system is safe, has high security, and does not easily lead to errors for other objects to penetrate (Tang *et al.*, 2008). Besides, decentralizing access rights or security when accessing to ensure privacy also increases customers' trust in online service providers. Decentralization will prevent access to private data (Radulescu, 2018) improperly.

Furthermore, four private information protected perception factors also directly affect customers' purchase intention. In which, unauthorized secondary use (internal) (β = 0.31, t-value = 7.892), and collection (β = 0.235, t-value = 5,708) strongly influence customers' online purchase intention. Beside, Improper Access (β = 0.207, t-value = 4.524), and Error (β = 0.234, t-value = 5.193) have also positive effect on the online purchase intention. Thus, all hypotheses from H5 to H8 are supported with a significant level of 1%. The influence of ICOPIP on purchase intention differs from its effect on online trust. Customers will have a higher purchase intention if they know that the business collects their information properly (Radulescu, 2018) and the business does not use the collected data for purposes other than sales purposes, such as advertising (Jibril *et al.*, 2020; Mardjo, 2019).

Finally, online trust was confirmed to impact online purchase intention positively (β = 0.161, t-value = 3.971); hence, hypothesis H9 was accepted. Customer trust has been proven to influence their purchase intention greatly. Online shoppers' trust in website-based e-commerce statistically affects customers' purchasing intentions (Khoa, 2021). A high level of trust leads to higher purchase intentions among internet customers (Alshare *et al.*, 2019).

6. Conclusion

Worldwide, but especially in Vietnam, e-commerce is rapidly expanding in popularity. Creating an online storefront is a goal of almost every retailer nowadays. Although consumers gain, there are risks associated with online shopping, especially regarding their private information. One may argue that the key to this kind of firm's success is ensuring its customers' confidentiality. Online safety concerns are a major roadblock to using the Internet as a promotional tool. Numerous studies show that customers' worries about the security and privacy of their transaction data discourage them from making purchases online. According to the experts, system security issues are the top concern of online buyers since other parties might snoop on their personal information. This instance demonstrates that purchasers lack confidence in online

vendors since they do not meet face-to-face like when buying and selling via conventional distribution methods. If clients' sensitive information is securely guarded and protected, the time it takes to create confidence in this paperless, face-to-face business environment will be much shorter.

This study has stated that a business's privacy information practice significantly impacts online customer trust and behavior. Specifically, if customers are well aware of the ability to enforce their privacy policies, they will increase their trust and lead to purchase intentions on e-commerce sites. In addition, businesses that implement good privacy protection policies also directly increase consumers' purchase intention.

To ensure the security of consumers' personal information, businesses must first act fairly and honestly in their operations, and their websites must provide an easily accessible part detailing the company's background and policies. Businesses need to safeguard their customers' privacy by giving them control over who can see their data, what they can see, and what they cannot see via individual accounts. The prevention of data loss is the goal of information security. However, to prevent client information exploitation, companies must employ a suitable security mode in customer transactions, record information on unusual activities and transactions in the system, and guide customers when providing information. E-commerce businesses must continuously improve their executives' management and professional skills to carry out these tasks effectively. Most importantly, these businesses' upper management must foster an environment where the security of their customer's personal information is consistently prioritized.

Legal issues like system policies, regulations, and human factors; organizational issues like auditing electronic data processing, management, and perception; and technical issues like cryptographic techniques, network security, and smart card technology make up the primary research domain of information security. Therefore, this study's findings may pave the way for future research that further investigates how information security affects the habits of online shoppers.

Acknowledgment

This study is being conducted with funding from the Industrial University of Ho Chi Minh City under Grant number 21.2TMDL01 (Contract for Scientific research and Technology development No. 26/HD-ĐHCN)

Reference

Accenture. (2018). Accenture technology vision 2018: Unleash the intelligent enterprise. Retrieved from https://www.accenture.com/au-en/insight-technology-trends-2018.

Alshare, K. A., Moqbel, M., & Al-Garni, M. A. (2019), The impact of trust, security, and privacy on individual's use of the Internet for online shopping and social media:

a multi-cultural study. I*nternational Journal of Mobile Communications,* 17(5), 513-536.

Belanger, F., Hiller, J. S., & Smith, W. J. (2002), Trustworthiness in electronic commerce: the role of privacy, security, and site attributes. *The Journal of Strategic Information Systems,* 11(3-4), 245-270.

Bock, G.-W., Lee, J., Kuan, H.-H., & Kim, J.-H. (2012), The progression of online trust in the multi-channel retailer context and the role of product uncertainty. *Decision support systems,* 53(1), 97-107.

Bricker, D., Fellow, C. S., Hampson, F. O., & Fellow, C. D. (2018). Internet Security and Trust. Retrieved from https://unctad.org/system/files/non-official-document/dtl_eweek2016_DBricker_FOHampson.pdf.

Carmines, E. G., & Zeller, R. A. (1979). Reliability and validity assessment. *Sage publications,* Beverly Hills, California.

Chang, Y., Wong, S. F., Libaque-Saenz, C. F., & Lee, H. (2018). The role of privacy policy on consumers' perceived privacy. *Government Information Quarterly,* 35(3), 445-459.

Conger, S., Pratt, J. H., & Loch, K. D. (2013). Personal information privacy and emerging technologies. *Information Systems Journal,* 23(5), 401-417.

Dehghani Soltani, M., Shoul, A., & Ramezani, S. (2019). Investigating environmental value and green image supposed effects on the word of mouth advertising tendency by explaining green trust and willingness to pay roles through the SOR model framework. *Journal of Business Management,* 11(4), 804-824.

Dennis, C., Jayawardhena, C., & Papamatthaiou, E.-K. (2010), Antecedents of internet shopping intentions and the moderating effects of substitutability. *The International Review of Retail, Distribution and Consumer Research,* 20(4), 411-430.

Dinev, T. & Hart, P. (2003). Privacy concerns and Internet use--a model of trade-off factors. Paper presented at the Academy of Management Proceedings, Briarcliff Manor, NY 10510. DOI: 10.5465/ambpp.2003.13792464.

Featherman, M. S., & Pavlou, P. A. (2003). Predicting e-services adoption: A perceived risk facets perspective. *International Journal of Human-Computer Studies,* 59(4), 451-474. DOI:10.1016/s1071-5819(03)00111-3.

Frik, A. & Mittone, L. (2019). Factors influencing the perception of website privacy trustworthiness and users' purchasing intentions: The behavioral economics perspective. *Journal of theoretical and applied electronic commerce research,* 14(3), 89-125.

Ha, H.-Y. & Janda, S. (2014). The effect of customized information on online purchase intentions. *Internet Research,* 24(4), 496-519. DOI:10.1108/IntR-06-2013-0107.

Hair Jr, J. F., Hult, G. T. M., Ringle, C., & Sarstedt, M. (2016). A primer on partial least squares structural equation modeling (PLS-SEM). *Sage publications*, Washington DC.

Hong, W., & Thong, J. Y. (2013), Internet privacy concerns: An integrated conceptualization and four empirical studies. *MIS quarterly,* 275-298.

Jibril, A. B., Kwarteng, M. A., Nwaiwu, F., Appiah-Nimo, C., Pilik, M., & Chovancova, M. (2020). Online identity theft on consumer purchase intention: A mediating role of online security and privacy concern. Paper presented at the Conference on E-Business, e-Services and e-Society.

Khoa, B. T. (2021). Trust based online food review toward customers' restaurant selection intention in food and beverage service. *Journal of Logistics, Informatics and Service Science,* 8(2), 151-170. DOI:10.33168/liss.2021.0209.

Lee, J., Park, D. H., & Han, I. (2011). The different effects of online consumer reviews on consumers' purchase intentions depending on trust in online shopping malls. *Internet Research,* 21(2), 187-206. DOI:10.1108/10662241111123766.

Lee, S. K., & Min, S. R. (2021). Effects of information quality of online travel agencies on trust and continuous usage intention: An application of the SOR model. *The Journal of Asian Finance, Economics and Business,* 8(4), 971-982.

Li, Y. (2011). Empirical studies on online information privacy concerns: Literature review and an integrative framework. *Communications of the association for information systems,* 28(1), 28.

Liu, C., Marchewka, J. T., Lu, J., & Yu, C.-S. (2005). Beyond concern—A privacy-trust-behavioral intention model of electronic commerce. *Information & management,* 42(2), 289-304.

Mardjo, A. (2019). Impacts of social media's reputation, security, privacy and information quality on Thai young adults' purchase intention towards Facebook commerce. *UTCC International Journal of Business and Economics,* 11(2), 167-188.

Mehrabian, A. & Russell, J. A. (1974). An approach to environmental psychology. *MIT Press,* Cambridge, Mass. ; London.

Mutimukwe, C., Kolkowska, E., & Grönlund, Å. (2020). Information privacy in e-service: Effect of organizational privacy assurances on individual privacy concerns, perceptions, trust and self-disclosure behavior. *Government Information Quarterly,* 37(1), 101413.

Preibusch, S. (2013). Guide to measuring privacy concern: Review of survey and observational instruments. *International Journal of Human-Computer Studies,* 71,(12), 1133-1143.

Radulescu, A. (2018). Users' social trust of sharing data with companies: online privacy protection behavior, customer perceived value, and continuous usage intention. *Contemp. Readings L. & Soc. Just.,* 10, 137.

Smith, Dinev, & Xu. (2011). Information privacy research: An interdisciplinary review. *MIS quarterly,* 35(4), 989-1016. DOI:10.2307/41409970.

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS quarterly,* 167-196.

Solove, D. J. (2007). I've got nothing to hide and other misunderstandings of privacy. *San Diego L. Rev.,* 44, 745.

Taddei, S. & Contena, B. (2013). Privacy, trust and control: Which relationships with online self-disclosure? *Computers in Human Behavior,* 29(3), 3, 821-826.

Tang, Z., Hu, Y., & Smith, M. D. (2008). Gaining trust through online privacy protection: Self-regulation, mandatory standards, or caveat emptor. *Journal of management information systems,* 24(4), 153-173.

Valdez, L. E. (2021). Socially responsible buyers' online trust on the website and their level of satisfaction. In *Handbook of Research on Reinventing Economies and Organizations Following a Global Health Crisis,* 80-97, IGI Global.

Yun, H., Lee, G., & Kim, D. J. (2019). A chronological review of empirical research on personal information privacy concerns: An analysis of contexts and research constructs, *Information & management,* 56(4), 570-601.

Zhang, X., Liu, S., Chen, X., Wang, L., Gao, B., & Zhu, Q. (2018). Health information privacy concerns, antecedents, and information disclosure intention in online health communities. *Information & management,* 55(4), 482-493.

Zhou, T. (2020). The effect of information privacy concern on users' social shopping intention. *Online Information Review,* 44(5), 1119-1133. DOI:10.1108/OIR-09-2019-0298.

Zhu, L., Li, H., Wang, F.-K., He, W., & Tian, Z. (2020). How online reviews affect purchase intention: a new model based on the stimulus-organism-response (S-O-R) framework. *Aslib Journal of Information Management,* 72(4), 463-488. DOI:10.1108/ajim-11-2019-0308.