Journal of Theoretical and Applied Information Technology
15th June 2020. Vol.98. No 11

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

RELATIONSHIP BETWEEN CUSTOMERS' ONLINE SHOPPING BEHAVIOR AND PERSONAL INFORMATION DISCLOSURE

[1]IN WANG, [2]JONGCHANG AHN

[1]Manager, Branch of Chongqing Province, China Merchants Bank, China

[2]Associate Professor, Department of Information Systems, Hanyang University, Republic of Korea

E-mail: [1]15922657719@163.com, [2]ajchang@hanyang.ac.kr (*corresponding author)

ABSTRACT

With the rapid development of the Internet and continuous improvement of the e-commerce platform, online shopping has gained popularity among customers in China. Consequently, protecting customers' personal information is of concern. However, previous studies have focused on self-disclosure of personal information unlike this study. This study addresses this problem and analyzes the main factors and means of personal information disclosure in the online shopping process through a stringent statistical process with a suitable sample size. It examines the impact of factors generated from related previous research on customers' personal information disclosure. Based on the research model, questionnaires are developed and a survey is conducted to collect sample data (n=370), targeting Chinese online shopping customers. The findings indicate that information significance and website reputation have a positive influence, whereas trust has a negative influence on protective behavior intention, which in turn negatively influences information disclosure. This study can contribute to research on customers' privacy protection and also the legal usage of customer information by shopping platform operators and sellers in the online shopping market.

Keywords: *Personal Information Disclosure, Protective Behavior Intention, Electronic Commerce, Privacy Protection, Online Shopping*

1. INTRODUCTION

With the fast development of the Internet and mobile technology, more and more people have begun to use the technologies for their ordinary lives, to sufficiently enjoy the convenience it brings. The Internet has developed revolutionary changes in our lives. People take into account it a reliable source of information about products and services [1]. In particular, online shopping—the emerging consumption pattern, with its advantages such as fair price, diversified goods, and attentive service—is meeting the needs of modern society [2]. E-commerce sites in China mainly comprise enterprises and individuals conducting B2C (Business to consumer) transactions, such as the online shop Tmall, C2C (Consumer to consumer) online platform TaoBao.

Along with providing people rich goods and convenient services, e-commerce also leads to the problem of personal information security. While internet marketing is perceived as a threat or nuisance by many customers, it is a useful tool for online and offline businesses. Rapid advances in information technology (IT) and the increase of internet use have enabled business firms to gather, classify, store, distribute, and trade consumer data that can be used for developing accurately targeted marketing. The recently discovered famous Chinese e-commerce sites Jingdong.com store and dangdang.com leaked their user data, which made network information security once again a hot topic of discussion (e.g., www.technode.com, 12/12/2016).

In the entire process of online shopping, from the initial information registration, logging in, to the last order, and finally, filling in the online

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

payment details, consumers are requested to provide personal information, such as name, gender, email address, and delivery address, and mobile phone number. In addition, some business firms also require consumers to provide monthly income, education, occupation, and other specific/unique personal information. Online payment also relates to payment account, credit card details, transaction password, and other personal property information. Therefore, consumer information integrity and confidentiality should be protected in the open-network environment.

This study aims to empirically test the relation between personal information disclosure and customers' online shopping behavior. Because previous studies in this regard are focused on self-disclosure of personal information unlike the present study. Online shopping behavior is categorized into four main classifications: information significance (IS), website reputation (WR), trust (TR), and protective behavioral intention (BI). This study analyzes the main factors affecting personal information disclosure in an e-commerce environment. All survey results are based on customer perspectives. In addition, the study provides initial evidence through a stringent statistical analysis result with a suitable sample size.

The next chapter presents a literature review and the research model based on the previous research. Based on a survey of 370 respondents, empirical analyses were conducted according to the research method. For the validity, reliability, correlation, and regression analyses of the survey results, SPSS 21.0 and AMOS 22.0 were used. Finally, this study analyzes and discusses several factors affecting consumers' information disclosure.

2. LITERATURE REVIEW

2.1 Development of E-commerce in China

With the global history of e-commerce development, the development of e-commerce in China also started from the Electronic Data Interchange (EDI) application. In 1990, China ex-cogitated the application of United Nations Electronic Data Interchange for Federal Administration Commerce and Transportation (UN/EDI FACT) standards, especially in international trade and related fields, and the application of EDI in foreign trade enterprises was achieved. By the end of 1995, when the Internet started to become a new wave, the network technology began to spread into every area of social life. Various business websites, internet companies, and e-commerce businesses began to be boosted on the basis of the very fast development of e-commerce in China [2].

From 1997 to 1998, China's e-commerce was the main area of some IT manufacturers and the social network sites. They were used in various ways to execute e-commerce enrichment education to stimulate and attract people's understanding, knowledge, and demand of e-commerce. Meanwhile, they promoted the introduction, development, and application of e-commerce technology, enabling China's e-commerce technology to keep up with the global trend in a very short time, and laid the foundation for further development in the future. In 1999, Chinese e-commerce started a new period characterized by the exploration and introduction of large-size e-commerce projects. In addition, the network service providers such as internet service provider (ISP) and internet content provider (ICP) entered the field of e-commerce, and new e-commerce websites and projects suddenly increased dramatically. Almost every day, all types of e-commerce information consulting websites, online stores, online shopping malls, and online auction sites emerged, e.g., 8848.com and eBay. With the development of B2C, C2C and B2B also had a constant start. In 1999, many e-commerce, commercial, and industrial enterprises began to plan business to business (B2B) e-commerce. For example, the Haier group and other large businesses began to apply e-commerce within other enterprises.

In July 2008, China became the world's largest internet population. According to CNNIC statistics, as of June 30 in 2008, the number of internet users in China registered 253 million, ranking first in the world. After 2003, e-commerce in China experienced a series of major events. For example, in May 2003, the Alibaba group founded Taobao, entering the C2C market. In January 2004, Jingdong entered in the field of e-commerce. Alibaba Network was successfully opened in Hongkong stock market in November 2007. At the same time, with the fast growth of number of internet users and amount of e-commerce transactions, e-commerce became a new channel for many enterprises and individuals [3].

In 2013, China became the world's largest online retail market surpassing the United States.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

The e-commerce transaction scale exceeded 10 trillion yuan and the amount of online retail transactions reached 1.85 trillion yuan. The rapid and enlarged development of e-commerce promoted the development of broadband, IT outsourcing, cloud computing, third-party payment, online marketing, online shop operators, express logistics services, and production services, and formed a huge e-commerce ecosystem. Recently, the growth rate of e-commerce transaction volume has continued to maintain rapid growth momentum. Particularly, (Tmall 11.11 shopping) Carnival Taobao's business volume reached as much as 120 billion yuan in 2016 [3]. Certainly, e-commerce is becoming an important driving factor and engine for promoting the rapid growth of national economy.

2.2 Importance of Personal Information Protection

New technology has enabled business firms to explore new vastly improved and exciting applications such as data mining, data warehousing, target marketing, and self-service [4]. With the advent of the big data and data mining, personal privacy and network security risk issues have become increasingly prominent. Online transactions pose several new threats, such as hacking into networks including hard drives, the placement of cookies, intercepting transactions, and observing online behaviors via spyware. Meanwhile, customer service and online marketing to the Internet also pose great burdens such as the emergence of severe privacy concerns and resulting negative consumer results. This kind of threat to consumer privacy posed by the Internet needs exigent attention as it may damage a business firm's marketing performance in the long term [5].

In the situation of network consumption, consumers in online transactions are always faced with personal information problems, including illegal collection, processing, trading, disclosure, and other security risks. It has become the main area of personal information violations and losses. Consumer's personal information may also be leaked or stolen because of insufficient technical precautions and untimely remedy of security vulnerabilities of network service providers including ISPs and ICPs.

While online information protection has caught the attention of the government, businesses, and the public, consumers' information is risky when they visit websites and/or conduct complete transactions online [6]. A report released by the China Consumer Association shows that 70% of consumers' disclosed personal information has been leaked. Personal information leakage/theft and illegal use of the industry have shown explosive growth and a considerable pecuniary loss.

When consumers shop online, more amounts of personal information move about in cyberspace [7]. This information can then be sold or traded between companies to obtain comprehensive information about a consumer. Personal information has become a commodity to be sold, bought, or traded. Profitability has become more significant than privacy [8,9]. Internet technology has made it very easy to gather vast amounts of personal information, with digital networks making it possible to link or connect all this information [10].

Additional threat to consumer privacy occurs after a company gets consumer's personal information. In some cases, companies have not kept their promise of not sharing the data with third parties. Therefore, consumers are also encouraged to install home firewall applications and virus protection software, be very careful of what information they hand out, and not download anything unless he or she trusts it.

2.3 Customers' Trust for Shopping Websites

E-commerce involves purchasing and selling of products or services through electronic systems such as the Internet and computer networks, which is a transaction through electronic trading rather than a face-to face transaction. Generally, in e-commerce transactions, the consumers first order what they need through an online platform and remit money to the online seller. The online seller then sends the goods to the consumer after receiving the remittance [2].

It has been reported that 10% of web users never provide their personal information for websites that require registration, resulting in a leakage of information gathered by the website owner/marketer [11]. In general, an internet marketing strategy focuses on a sustainable relation and a series of business transactions with several customers. This strategy becomes possible through the acquisition of information regarding customers' purchasing patterns, commodity preferences, and personal information. These e-commerce website databases, however, require various consumers to share their personal information or privacy

voluntarily or involuntarily. In most cases, e-commerce needs consumers to publish a certain amount of personal information (e.g., name, e-mail address, and phone number) and payment information (e.g., credit card account and password). However, consumers have generally shown increasing concerns over privacy problem due to an increase in doubtful and illegal activities on the Internet, such as a rise in spam and spyware, identity theft, and hacking.

A survey presented that only 24.9% of consumers perceived comfortable in using their credit card for buying goods on the Internet [12]. Thus, issues of security and privacy in e-commerce have been attracting research attention in different fields. Consumers' increased concern over their personal information is a pivotal problem for the potential growth of e-commerce. The proliferation of social (media) technologies has been viewed as a desirable change in the way people discuss/communicate, share information, collaborate, transact online, and consume [2].

2.4 Characteristics of Personal Information in Electronic Commerce

The "right to privacy" has promoted considerable discussion in many fields including law, sociology, politics, philosophy, and more recently, information systems and computer science. In addition, how the right to privacy fares when applied to the sphere of e-commerce is an even more problematic and argumentative question [13].

(1) Specifically, personal information in e-commerce refers to the information collected during online trading process. Consumers provide their name, e-mail address, contact information, credit card number, and other required information to complete the transaction, which is also a field of personal information in e-commerce [14]. That is, only the individual information of consumer behavior in e-commerce belongs to the category of personal information in e-commerce.

(2) In the e-commerce situation, personal information seems to be more valuable. Because consumers will self-disclose their personal information to the e-commerce firm in the transaction process, enterprises can get information to calculate the consumer demand and achieve considerable commercial value. Therefore, under the threat of criminals or thieves targeting consumer information, it is particularly essential to protect customer's personal information.

2.5 Privacy Concerns of Consumers

It is commonly known that privacy is difficult to define [15]. Internet retailers use the electronic market-space information to build positive relationships with consumers. Consumers' privacy concerns about the weakening or loss of control over their information may reduce the relationships, ultimately affecting the consumers' decision to repurchase online.

The Internet has heightened various consumer concerns regarding privacy [16]. Specifically, consumers' dread includes an increase in the number of website databases, the vast volume of personal information that is being gathered, and the higher possibility of privacy intrusions and loss of control in the process of gathering, accessing, and exploiting this information [17]. Faced with these concerns, consumers sometimes do behaviors such as providing wrong or fabricated information to a shopping website, installing their computers to reject cookies and spam, or avoiding purchase goods from particular websites [18]. Eventually, these possibly negative reactions emerging from threats to consumer privacy would have a substantial impact on a company's marketing performance.

In general, the invasion of privacy on the Internet is regarded as an unauthorized gathering, disclosure, or other usage of personal information [19]. Even before the Internet era, a consumer's personal information was often collected, stored, analyzed, and exchanged for multiple marketing purposes such as direct marketing (DM) and telemarketing. However, before e-commerce, consumer transactions provided a natural protection to consumer's personal information, particularly where transactions were conducted in cash and consumers avoided handing out personal information. Therefore, when a transaction occurs on the Internet, consumers should be particularly protective of their privacy [20, 21, 22, 23]. However, previous studies in this regard are focused on self-disclosure of personal information unlike the present study.

3. RESEARCH MODEL

3.1 Research Hypothesis Development

Information Significance: The importance of information says users' attention to a certain type of data in a specific situation as discussed above [24]. In this paper, the definition of personal information includes e-mail, cell phone number, address, credit

card account, and ID card information. In other words, the significance of the information is how much attention consumers pay to these five types of personal information to protect their privacy.

Through a survey conducted by a previous study [25], it was found that the proportion of internet users having the intention to provide their personal tastes and mailboxes reached 82% and 76%, respectively, whereas only 3% expressed willingness to provide credit card details. In addition, the more internet users were willing to provide their demographic characteristics and shopping preferences (habits) than financial information and ID information.

Therefore, this study suggests that the more attention consumers pay to the information, the lower is the probability of information leakage.

Hypothesis 1: Information significance will have a positive influence on protective behavior intention.

Website Reputation: This is the evaluation regarding the quality of business products and services that consumers reflect in their shopping experience, as well as a sign of the impact of the site [26]. A research has found that Amazon's reputation is an important factor influencing its sales [27]. The statistical study also found that a good reputation in the B2C exchange relationship can increase the willingness of consumers to submit personal information and execute transactions [6].

Thus, the site's reputation influences the consumer's intention to purchase, while the reliability of an undesirable site may be a cause of consumer information security. In this study, the two factors that are considered to influence the reputation of a website are the website's popularity and public praise. Therefore, this study suggests that selecting a reputable website is helpful to the protection of personal information.

Hypothesis 2: Website reputation will have a positive influence on protective behavior intention.

Trust: This is important in relationship setting and building. It contributes to satisfaction and sustainable association over and beyond the effects of the financial results of the relationship [28]. In the e-commerce environment, in general, trust is defined as the extent to which consumers believe that the e-commerce sites can protect their privacy. Excessive trust of consumers in the shopping website is also likely to bring about privacy disclosure [29]. Because of the uncertainty and risks to e-commerce, trust has become an important factor influencing consumer's personal information and purchase intention.

This paper assumes that a consumer's trust in a shopping website includes over-reliance on the website, how personal information is used by the website, and trust of the website's commitment to protect privacy, as well as the trust of whether they will share the information with, or sell to, third parties.

Therefore, this study suggests that excessive trust of a consumer on a shopping site causes leakage of personal information.

Hypothesis 3: Trust will have a negative influence on protective behavior intention.

Protective Behavior Intention: E-commerce based on the online economy must conduct the transaction based on the consumer's personal information, which provides consumers for convenience. However, it also can be a potential threat to their privacy and security.

Previous studies have shown that the main factor influencing the adoption of e-commerce by consumers is a threat to privacy and security, where most consumers mentioned that the reason for offline shopping is fear of personal privacy leaks [30]. The privacy concerns of American consumers are found to negatively impact their willingness to provide personal information to web sites, their willingness to engage in e-commerce transactions, and even their willingness to surf the Internet [31]. Therefore, the consumer's attention to privacy will influence an individual's intention to protect privacy.

This study presents that the protective behavior intention of consumers in online shopping for their own information protection includes the following: installing an appropriate software to prevent the third party threat to personal information; paying deep attention to personal information and privacy protection policies in standpoint of email encryption; regular clean-up of browsing records; and correct disposal of the express list.

Therefore, this study suggests that the lower the consumer's awareness for personal information

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

protection, the higher is the possibility of information leakage.

Hypothesis 4: Protective behavior intention will have a negative influence on information disclosure.

3.2 Research Model

Based on previous studies and investigations, this paper selects four main factors influencing consumer information disclosure (ID) as research hypothesis development: IS, WR, TR, and BI. IS is defined as the degree of attention a consumer pays to their own information and comprises five subparts: phone number, address, credit card, email, and identity information [14, 24]. WR includes the choice of high-credit and reputable websites [6]. TR involves customer trust in the use of website information and information protection [32]. BI embraces consumers' installation of anti-virus software, clear records, and other self-protection behavior [33]. In general, ID can be brought about during the online shopping, logistics, and website browsing processes [6]. The research model is shown in Figure 1.

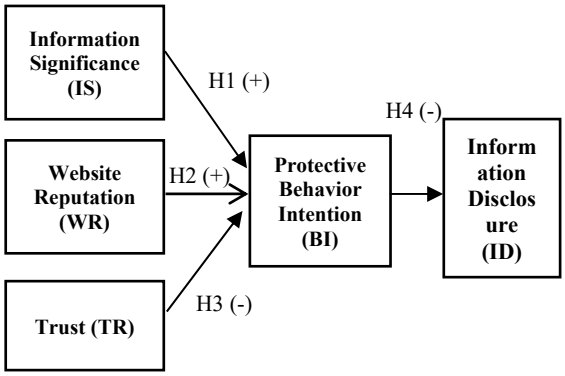

Figure 1: Research Model

4. RESEARCH METHOD AND ANALYSIS

4.1 Research Method

This study includes creating a theory and developing a method to test the hypotheses including actual collection of data. The research objectives can be concluded as identifying customers' possible online behaviors that lead to the disclosure of personal information. In this paper, a wrong choice of sites, excessive trust, and weak awareness of protection are hypothesized as the main behaviors that have positive impacts on information disclosure.

To investigate the main factor of information disclosure, this study collected sample data from the general public that has online shopping experience. The survey was conducted through Sojump.com (the most functional survey website in China). In May 2017, 370 responses were collected to be used as data for the main empirical analysis.

The survey includes six parts of questions, five on demographic data, five on information significance, two on site selection, five on trust, four on behavioral intention, and three on information disclosure. This survey includes the questions on selecting the website of subjects' information disclosure experiences, protective perspectives, and the questions of demographic information. Optional answers are classified into (1) strongly disagree, (2) disagree, (3) neither agree nor disagree, (4) agree, and (5) strongly agree.

4.2 Data Analysis and Results

For analyzing the survey results, IBM SPSS Statistics 21.0 and AMOS 22.0 were used. The validity, reliability, and correlation analyses of variables are shown below.

The sample's demographic characteristics are shown in Table 1. The study sample has the following characteristics: gender is slightly unequally represented, with males outnumbering females. The sample mainly comprises people under the age of 30, their proportion being 70%. In terms of education background, undergraduate college or above account for 81.02%. Monthly income is mainly in the middle and low income group, which is related to the respondents being mainly college students. At present, China's internet users of 20−30 age group account for the largest proportion of online shopping customers, comprising mainly of college students. Therefore, the sample can be used for e-commerce consumers' personal information disclosure.

The reliability of the measurement tool presents of how well the items for one construct correlate or move together [34]. The reliability of a research measurement tool concerns the extent to which the instrument presents the same results in repeated trials. The tendency toward consistency found in repeated measurements/trials is called as reliability [35].

Cronbach's alpha value is a measure of internal consistency among all items utilized for one

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

construct. Reliability is usually tested by two indicators/tools—Cronbach's alpha and composite reliability (CR), which states a similar concept, but the former is considered a stricter reliability measure in the context of structural equation modeling (SEM) [36]. In this study, the Cronbach's alpha value is commonly used as a measure of internal consistency to reliability concept. The Cronbach's alpha coefficients of each index are shown in Table 2. They are more than 0.8, and one of them had the value more than 0.9, indicating good and high reliability of the measurement for each construct [37].

Table 1: Demographic statistics of respondents.

Demographic variables	Category	Number of people	Percentage
Gender	Male	214	57.84%
	Female	156	42.16%
Age	<18	5	1.35%
	18--30	254	68.65%
	31--40	32	8.65%
	41--50	52	14.05%
	≥51	27	7.3%
Highest education	High school and below	17	4.59%
	Junior college	54	14.49%
	Undergraduate college	162	43.78%
	Master's Degree Candidate	113	30.54%
	Doctoral candidate and above	24	6.49%
Monthly income (RMB)	<2000	184	49.73%
	2000--4000	32	8.65%
	4001--6000	61	16.49%
	6001--8000	36	9.73%
	8001--10000	28	7.57%
	≥10001	29	7.84%
Credit card having	Yes	202	54.59%
	No	168	45.41%

Validity is defined as the degree to which a test measures what it is supposed to measure. In the statistical area, there are basic approaches to validating the tests and measures including content validity, construct validity including several sub-validity concepts [38].

Construct validity is evaluated with convergent validity and discriminant validity. Convergent validity is defined as the degree to which the measurement (observed) items are relevant to the construct (variable), and theoretically, they are predicted to be related [34]. Factor analysis is an approach searching a way of condensing the information containing several initial variables into a smaller set of factors (dimensions) with a minimum loss of information. Since each factor loading value on each construct is more than 0.5, the convergent validity for each scale is established [39]. Table 2 shows that the factor loading of each construct is over 0.7, with some having reached over 0.9.

Discriminant validity is defined as the degree to which measures of different constructs are distinct [39]. CR and average variance extracted (AVE) are presented in Table 2, where the CR of all factors is more than 0.8 and AVE is above 0.5. To test the discriminant validity, correlations between the construct and other items in the model and the square roots of the AVE are compared.

Table 2: Factor loading, Cronbach's alpha, CR, and AVE

Variables	Questions	Factor loading	Cronbach's Alpha	CR	AVE
IS	IS1	.901	0.925	0.942	0.767
	IS2	.865			
	IS3	.851			
	IS4	.887			
	IS5	.867			
WR	WR1	.874	0.895	0.895	0.811
	WR2	.927			
TR	TR1	.771	0.883	0.925	0.712
	TR2	.821			
	TR3	.821			
	TR4	.886			
	TR5	.815			
BI	BI1	.704	0.839	0.839	0.575
	BI2	.815			
	BI3	.768			
	BI4	.738			
ID	ID1	.914	0.895	0.898	0.747
	ID2	.806			
	ID3	.867			

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 3 present the correlations and each construct's AVE. The diagonal values (bold numbers) are the square roots of the AVE, all of which are higher than the correlation values. Therefore, all items in this research fulfill the requirement of discriminant validity.

In this study, using the confirmatory factor analysis (CFA), the five constructs are allowed to freely correlate. The CFA provides proofs for a close/high fit between the measurement model and the data. Putting all indicators together, the measurement model had a satisfactory quality in standpoints of construct validity, discriminant validity, and reliability.

Table 3: Discriminant validity of constructs

	IS	WR	TR	BI	ID
IS	**0.875**				
WR	0.547	**0.901**			
TR	-0.582	-0.457	**0.843**		
BI	0.558	0.477	-0.559	**0.758**	
ID	-0.378	-0.229	0.306	-0.208	**0.864**

In this study, using IBM AMOS 22.0, the method of maximum likelihood estimation (MLE) is used to test the fitness of the main model. The evaluation criteria of each index are presented in Table 4, where the main model has a good fitness level with the sample data, which can be used to verify the above four hypotheses.

Several fit indices are used to evaluate the fit of the model, including goodness of fit index (GFI), adjusted goodness of fit index (AGFI), normed fit index (NFI), comparative fit index (CFI), and root mean square error of approximation (RMSEA). The fit indices evaluate the model's fitness for the data being examined. They can determine which proposed model best fits the data, by presenting how well the parameter estimates the account for the observed co-variances. The models demonstrate two main types of fit: overall fit (chi-squared test, GFI, AGFI, NFI, CFI, and RMSEA) and local fit of individual parameters [40].

Chi-square is the traditional test of fitness degree in SEM, which evaluates the magnitude or extent of discrepancy between the sample and the fitted co-variance matrices [41]. Many researchers have recommended more than 0.90 as a valid and appropriate criterion for determining adequate model fit for the indices of GFI, AGFI, NFI, and CFI [42]. However, for CMIN/DF and RMSEA, they consider each lower 3.0 and lower 0.08 value as the appropriate criterion for fitness. Table 4 shows that all fit indices indicate a good model fit for the sample size.

Table 4: Model fitting test

Index	Evaluation criterion	Fitting value	Model fitness
CMIN/DF	<3.0	1.653	√
GFI	>=0.90	0.935	√
AGFI	>=0.90	0.915	√
NFI	>=0.90	0.978	√
CFI	>=0.90	0.982	√
RMSEA	<0.08	0.042	√

To test Hypotheses H1−H4, this study further applies SEM by AMOS 22.0 to generate an appropriate structural model. In this study, SEM method is used because this procedure allows modeling relations among a set of constructs, sufficient estimation of all hypothesized paths, and estimation of the extent of indirect or mediating effects [42].

H1 hypothesizes the existence of a positive relation between information significance and protective behavior intention. Specifically, the path coefficient for IS to BI is 0.236 and this relation is significant (t-value = 4.242, $p < 0.001$), so H1 is supported.

H2 proposes the existence of a positive relation between website reputation and protective behavior intention. The path coefficient for WR to BI is 0.157 and this relation is significant (t-value = 2.948, $p < 0.01$). Thus, H2 is also supported.

H3 argues the existence of a negative relation between customer trust and protective behavior intention, the path coefficient for TR to BI is -0.330 and this relation is significant (t-value = -4.919, and $p < 0.001$). Thus, H3 is supported.

H4 states the existence of a negative relation between protective behavior intention and information disclosure, and the path coefficient for BI to ID is -0.302 and this relation is also significant (t-value = -4.218, and $p < 0.001$). Thus, H4 is also supported. The results of hypothesis testing are shown in Table 5.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 5: Path analysis

Path	Standardized path coefficient	S. E.	T value	P value	Support or not
IS→BI	0.236	0.056	4.242	***	Support
WR→BI	0.157	0.053	2.948	**	Support
TR→BI	-0.330	0.067	-4.919	***	Support
BI→ID	-0.302	0.072	-4.218	***	Support

*** *p*-value < 0.001, ** *p*-value < 0.01

5. DISCUSSION AND CONCLUSION

5.1 Theoretical Implications

China has become the leader of e-commerce market in Asia and around the globe, with so many online shopping platforms or websites operating and serving for Chinese consumers. However, under the internet and electronic shopping mode, the problem of consumer's personal information disclosure is becoming increasingly emergent and prominent. The disclosure of consumers' personal information brings about great trouble to consumers' ordinary life but also severely influences the healthy and orderly development of online shopping environment. Therefore, from customer's perspective, it is very important and imminent issue to find out the main factors that cause the leakage or loss of personal information.

This study aims to investigate the relation between customers' personal information disclosure and online shopping behavior, in order to establish a consensus among them. The survey data used in this study originated from 370 respondents of a questionnaire developed on Sojump.com. As presented by the study findings through the strict statistical criteria and analyses, most online customers have deep concerns about their personal information while shopping on the Internet but also the security of identity and confidentiality. Therefore, consumers should be particularly protective of their privacy. However, previous studies are mainly focused on self-disclosure of personal information unlike the present study.

Based on the responses of those who participated in this survey, the vast majority of respondents prefer the websites with good reputation to have policies for internet use and personal information, as well as to notify the customers of the policies. Such policies and consumer's awareness would relieve prior risks and liability. However, previous studies in this regard have focused on self-disclosure of personal information unlike this study.

This study's findings suggest that government agencies should take into account establishing specific and comprehensive policies regarding customer's personal information issues in e-commerce, which can clearly notify customers of the purpose of information gathering, storage and use of information, and promise of no unauthorized disclosure of information to the third party. Under such policies, a certificate can be conferred to a compliant e-commerce. In this way, consumers would become less reluctant to conduct transactions on the Internet, thereby supporting the expansion and development of e-commerce.

Second, e-commerce websites should have a more professional design and be in the process of daily operation and supervision to establish a good brand image. In addition, the website should be used under reliable encryption and security technology, so another malicious acquisition of consumer information protection will not be there. Concretely, users should be reminded repeatedly to take tools to improve privacy protection and prevent or reduce the account information leakage risk.

5.2 Limitations and Further Research

This study has a few limitations. First, most of the sample respondents were regular or daily internet users. Thus, the results might not be generalized to those who are unfamiliar with online shopping. The use of a random representative sample, which is an option for future research, may provide different results. Second, most of the respondents were students or clerical workers, and thus, the results may not be generalized to other populations. Consumers can behave variously when making purchase decisions and buying concerning specific websites or product categories. However, too specific research may be difficult from the applicability of results to a wider range of situations.

The present study raises other questions that require further research. First, further research can be based on the survey of customers around the world, rather than being confined to Chinese customers. Second, future studies might measure actual disclosure rather than customers' behavioral

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

intention of disclosing personal information. Third, considering the variety of websites around the globe, customers' personal information protection behaviors can be analyzed and compared among various categories/groups of websites or online stores with different attributes. For example, the other B2B or C2C websites and other commercial websites can have different circumstances.

REFRENCES:

[1] B. Gervey and J. Lin, "Obstacles on the Internet: a new advertising age survey finds privacy and security concerns are blocking the growth of e-commerce." *Advertising Age*, Vol. 71, No.113, 2000.

[2] K.C. Laudon and C.G. Traver, E-commerce 2017- business technology. Society, 13th global ed. Pearson, 2017.

[3] iResearch: Survey report of Chinese online shopping industry—Part of currency and trend 2016, http://www.iresearch.com.cn/report/2945.html.

[4] C. Lovelock and J. Wirtz, Services marketing: people, technology, strategy. Library of Congress Cataloging-in-Publication Data, 2006, pp. 32−58.

[5] C. Gauzente and A. Ranchhod, "Ethical marketing for competitive advantage on the internet," *Academy of Marketing Science Review*, Vol. 1, No. 10, 2001, pp. 1−7.

[6] G.R. Milne, A.J. Rohm and S. Bahl, "Consumers' protection of online privacy and identity," *Journal of Consumer Affairs*, Vol. 38, No.2, 2004, pp. 217−232.

[7] A.B. Carroll, "Corporate social responsibility," *Business and Society*, Vol. 38, No. 3, 1999, pp. 268−295.

[8] D. Gillmor, "Violating privacy is bad business," *Computer World*, Vol. 32, No. 12, 1998, pp. 38−39.

[9] J. Kakalik and M. Wright, "Responding to privacy concerns of consumers," *Review of Business*, Vol. 18, No.1, 1996, pp. 15−18.

[10] P.R. Prabhaker, "Who owns the online consumer?" *Journal of Consumer Marketing*, Vol. 25, No. 4, 2000, pp. 329−346.

[11] C. Kehoe, J. Pitkow and K. Morton, GVU's 8th WWW user survey. Atlanta, GA: Graphic, Visualization, and Usability Center, Georgia Tech Research Center, 1997.

[12] T.R. Graeff and S. Harmon, "Collecting and using personal data: consumers' awareness and concerns," *Journal of Consumer Marketing*, Vol. 19, No. 4, 2002, pp. 302–318.

[13] M. Guo, "A comparative study on consumer right to privacy in e-commerce," *Modern Economy*, Online, 2012, pp. 402−407.

[14] Z. Zhang and Y. Zhang, "How do explicitly expressed emotions influence interpersonal communication and information dissemination? A field study of Emoji's effects on commenting and retweeting on a microblog platform," *20th Pacific Asia Conference on Information Systems*, *PACIS 2016 Proceedings*, Chiayi, Taiwan, June 2016.

[15] H.J. Smith, S.J. Milberg and S.J. Burke, "Information privacy: measuring individuals' concerns about organizational practices," *MIS Quarterly*, Vol. 20, No.2, 1996, pp. 167−196.

[16] E.M. Caudill and P.E. Murphy, "Consumer online privacy: Legal and ethical issues," *Journal of Public Policy & Marketing*, Vol. 19, 2000, pp. 7−19.

[17] M. Culnan, "How did they get my name? An exploratory investigation of consumer attitudes toward secondary information use," *MIS Quarterly*, Vol. 17, No. 3, 1993, pp. 341−362.

[18] M.J. Culnan and G.R. Milne, "The Culnan-Milne Survey on Consumers & Online Privacy Notices: Summary of Responses," *Inter-agency Public Workshop*, Get Noticed: Effective Financial Privacy Notices, Washington, D.C., 2001.

[19] H. Wang, M.K.O. Lee and C. Wang, "Consumer privacy concerns about Internet Marketing," *Communication of the ACM*, Vol. 41, No. 3, 1998, pp. 63−70.

[20] L. Wang, J. Yan, J. Lin and W. Cui, "Let the users tell the truth: Self-disclosure intention and self-disclosure honesty in mobile social networking," *International Journal of Information Management*, Vol. 37, No.1 (Part A), 2017, pp. 1428−1440.

[21] F. Belanger, J.S. Hiller and W.J. Smith, "Trustworthiness in electronic commerce: the role of privacy, security, and site attributes," *The Journal of Strategic Information Systems*, Vol. 11, No. 3-4, 2002, pp. 245-270.

[22] A.N. Joinson, U. Reips, T. Buchanan and C.P. Schofield, "Privacy, trust, and self-disclosure online," *Human Computer Interaction*, Vol. 25, No. 1, 2010, pp. 1-24.

[23] C. Nam, C. Song, E. Lee and C.I. Park, "Consumers' privacy concerns and willingness to provide marketing-related personal

information online," *NA - Advances in Consumer Research*, 33, eds. Connie Pechmann and Linda Price, Duluth, MN: Association for Consumer Research, 2006, pp. 212-217.

[24] R.J. Weible, Privacy and data: an empirical study of the influence and types and data and situational context upon privacy perceptions, US: Mississippi State University, 1993.

[25] L.F. Cranor, J. Reagle and M.S. Ackerman, Beyond concern: Understanding net users' attitudes about online privacy. Cambridge, MA: MIT Press, 2000:14, 1999.

[26] M.A. Eastlick, S.L. Lotz and P. Warrington, "Understanding online B-to-C relationships: An integrated model of privacy concerns, trust, and commitment," *Journal of Business Research*, Vol. 59, 2006, pp. 877−886.

[27] S.J. Barnes and R.T. Vidgen, "An integrative approach to the assignment of e-commerce quality," *Journal of Electronic Commerce Research*, Vol. 3, No. 3, 2002, pp. 114–127.

[28] N.K. Malhotra, S.S. Kim and J. Agarwal, "Internet users' information privacy concerns (IUIPC): the construct, the scale, and a causal model," *Information Systems Research*, Vol. 15, No.4, 2004, pp. 336−355.

[29] S. Taddei and B. Contena, "Privacy, trust and control: Which relationships with online self-disclosure?" *Computers in Human Behavior*, Vol. 29, No. 3, 2013, pp. 821−826.

[30] G.J. Udo, "Privacy and security concerns as major barriers for e-commerce: a survey study," *Information Management & Computer Security*, Vol. 9, No. 4, 2001, pp. 165−174.

[31] S. Bandyopadhyay, "Antecedents and Consequences of Consumers' Online Privacy Concerns," *Journal of Business & Economics Research,* Vol. 7, No. 3, 2009, pp. 41-48.

[32] J. Fogel and E. Nehmad, "Internet social network communities: Risk taking, trust, and privacy concerns," *Computers in Human Behavior*, Vol. 25, No. 1, 2009, pp. 153−160.

[33] C. Liu, J.T. Marchewka, J. Lu and C.S. Yu, "Beyond concern: a privacy-trust-behavioral intention model of electronic commerce," *Information & Management*, Vol. 42, No. 1, 2004, pp. 127−142.

[34] D. Straub, M.C. Boudreau and D. Gefen, "Validation guidelines for IS positivist research," *Communications of the Association for Information Systems*, Vol. 13, 2004, pp. 380−427.

[35] E.G. Carmines and R.A. Zeller, Reliability and Validity Assessment. Newbury Park, CA: Sage Publications, 1979.

[36] W.W. Chin, "The partial least squares approach for structural equation modeling," *Methodology for business and management*, G.A. Marcoulides (Ed.), Modern methods for business research (pp. 295-336). Mahwah, NJ, US: Lawrence Erlbaum Associates Publishers, 1998.

[37] J. Nunnaly, Psychometric theory, New York: McGraw-Hill, 1978.

[38] E. Manson and W. Bramble, Understanding and conducting research, USA: McGraw-Hill, 1989.

[39] J.F. Hair, W.C. Black, B.J. Babin, R.E. Anderson and R.L. Tatham, Multivariate data analysis. New York, NY: Prentice-Hall International, 2006.

[40] P. Bentler and E. Wu, EQS/windows user's guide. Los Angeles: BMDP Statistical Software, 1993.

[41] T.D. Smith. and B.F. McMillan, "A Primer of Model Fit Indices in Structural Equation Modeling," *Annual Meeting of the Southwest Educational Research Association*, New Orleans, LA, February 1-3, 2001.

[42] K. Bollen and J. Long, Testing structural equation models. Newbury Park, CA: Sage Publications, 1993.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Appendix: Questionnaire items for each construct

Construct	Item
Information significance (IS)	IS1: I will not provide my email to the website when I buy something online. IS2: I will not provide my cell-phone number to the website when I buy something online. IS3: I will not provide my address to the website when I buy something online. IS4: I will not provide my credit card number to the website when I buy something online. IS5: I will not provide my ID card information to the website when I buy something online.
Website reputation (WR)	WR1: I prefer to choose a better reputation and more well-known website to buy goods. WR2: I prefer to choose a website with high credit rating to buy goods.
Trust (TR)	TR1: I do not think most of China's e-commerce websites is trustworthy. TR2: I do not believe that e-commerce sites can abide by the commitment to protect privacy of customers. TR3: I think it is important how my personal information is used by websites. TR4: When I need to fill in my personal information, I will think it over and fill it out. TR5: When I provide personal information to the shopping site, I will worry about it for other purposes.
Behavioral intention (BI)	BI1: I set up my browser to reject unnecessary cookies and encrypt my e-mail. BI2: I always look for and read privacy policies of personal information protection. BI3: When I find out that my personal information is leaked, I will consider taking appropriate legal means. BI4: I have installed the corresponding software to prevent third party access to personal information or privacy.
Information disclosure (ID)	ID1: In the online shopping process my personal information has been leaked. ID2: In the logistics process my personal information has been leaked. ID3: In the website browsing process my personal information has been leaked.
Demographic questions	What is your gender? 1) Male 2) Female What is the highest degree or level of school you have completed? 1) High School and Below 2) Junior college 3) Undergraduate college 4) Master Degree Candidate 5) Doctoral candidate and above What is your age? 1) Under 18 years old 2) 18~30 years old 3) 31~40 years old 4) 41~50 years old 5) 51 years old or older How much is your current monthly income? 1) Under ￥2,000 2) ￥2,001~￥4,000 3) ￥4,001~￥6,000 4)￥6,001~￥8,000 5) ￥8,001~￥10,000 5) Over ￥10,001 Do you have credit card? 1) Yes 2) No