Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 14 / ISSUE 2 / MAY 2019 / 59-69

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762019000200106

Role of Privacy Legislations and Online Business Brand Image in Consumer Perceptions of Online Privacy Risk

Edward Shih-Tse Wang

National Chung Hsing University, Graduate Institute of Bio-Industry Management, Taichung, Taiwan, shihtse.wang@msa.hinet.net

Received 21 November 2017; received in revised form 25 April 2018; accepted 27 May 2018

Abstract

Developing an approach to manage privacy risk is critical to the success of e-marketing. Understanding the antecedents of privacy risk is therefore essential for the success of e-business. Because governments, businesses, and consumers are economic agents, this study examined the effects of governmental (privacy legislations) and firm-related (online business brand image) factors on consumer perceptions of online privacy risk. This paper proposes a conceptual model for exploring the underlying mechanisms of privacy legislations and online business brand image on consumer perceptions of online privacy risk. To test the conceptual model, data were collected from 425 students on a university campus which provided real personal information to online businesses within the preceding 3 months. Structural equation modeling was employed to test all the hypotheses in the conceptual model. The results reveal that perceived effectiveness of privacy legislations and online business brand image positively affect trust in online businesses. In addition, trust in online businesses positively affects perceived effectiveness of business privacy policies and perceived benefits of information disclosure, which in turn negatively influences online privacy risk perception.

Keywords: Perceived effectiveness of privacy legislations, Brand image, Trust in online businesses, Perceived effectiveness of privacy policy, Perceived benefits of information disclosure, Perceived privacy risk

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 14 / ISSUE 2 / MAY 2019 / 59-69

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762019000200106

1 Introduction

To facilitate service processes and management effectiveness, many online businesses encourage new consumers to provide personal information or preferences [5] to enable the provision of services tailored to consumers' specific needs [48]. However, personal information disclosure processes for consumers have raised privacy concerns [59] and privacy risk perceptions [17], [35], [54], [62]. Because personal data security is a major concern for consumers during online activities [22], information privacy has become a major challenge for online businesses in terms of collecting and efficiently utilizing data [52]. Perceived privacy risk is a key factor discouraging consumers from disclosing information [39] and one of the most negative factors in e-tailing [29]. Moreover, numerous studies have found that privacy concerns and privacy risk perceptions positively affect consumers' lurking behavior and self-concealment [51]. Privacy risk perceptions also negatively affect consumers' willingness to provide personal information [15], [28], [39] and to use online services [20], [21], [68], [69], thereby eventually leading to losses for online businesses [60] and exerting a considerable negative effect on online business performance [59]. Thus, because of the increasing importance of e-marketing and growing concerns regarding online privacy protection [6], the role of privacy risk in e-marketing is more crucial than ever before. Because of its rapid growth, e-marketing is crucial for exploring the antecedent variables of privacy risk to reduce consumers' online privacy risk concerns. Some studies have focused on the role of consumer characteristics such as age and gender [21] and previous experience of online disclosure [50], [63], whereas others have focused on providing personal information characteristics such as information sensitivity [16]. Furthermore, studies have explored the role of product characteristics such as perceived benefits of service use [10], [16] and compatibility [21] in privacy risk perceptions. Other studies have observed the effects of social influence [20], trust in service providers [20], [39], [50], [63], [68], [69], perceived justice [70], perceived exchange fairness [41], and perceived control [39] on perceived privacy risk.

Consumers, firms, and governments are economic agents [49]. Government and firm policies should affect consumer beliefs and behavior. Researchers have suggested that privacy legislation aims to provide a balancing force between commercial enterprises' collection of data that meet market needs and individual privacy protection [1]. Furthermore, a firm's privacy policy is a statement informing consumers how their information will be collected, used, and disclosed by the firm [40]. Online providers have been used to increase consumers' trust and willingness to disclose private information online [7]. Previous studies have indicated that regulatory expectations [16] and firm privacy policies [62] affect consumer privacy risk perceptions. Privacy legislations and business policies can reduce consumer privacy concerns [59]. In addition to these findings and their insights into online privacy risk, other empirical studies have focused on the direct effects of the aforementioned variables on perceived privacy risk. Little is known about whether mediators exist in the effects of these variables on perceived privacy risk; little attention has been devoted to gaining a comprehensive understanding of the gradational influence of these variables on perceived privacy risk. Moreover, exploring the antecedent variables of perceived privacy risk from various perspectives requires an enhanced understanding of how to reduce privacy risk concerns.

Branding is a unique tool for retailers because strong brands minimize perceived risk from a consumer perspective [13]. Studies have indicated that a credible brand increases consumer confidence and minimizes risk perceptions [36]. Branding provides a product with a reputation, thereby serving as a risk-reduction mechanism [45]. Kim and Kim [37] indicated that a strong service brand can reduce perceived purchase risks among consumers. Thus, the image of a store brand may influence consumers' risk perceptions regarding retail products. Although the findings of one previous study suggested that perceived risk is related to store reputation and brand recognition [2], few studies have empirically examined the association between online brand image and privacy risk perception. In summary, the present study examined whether and how privacy legislation and online business brand image have a gradational effect on consumer privacy risk perceptions. Because privacy risk is critical to the success of e-marketing, understanding the antecedents and underlying gradational influence mechanisms of privacy risk is essential. Without a comprehensive understanding of the factors affecting consumer risk perception and its underlying mechanisms, online business marketers face difficulty in inhibiting consumer privacy risk perceptions. The findings of this study can provide a reference for online businesses in developing effective programs for collecting consumer information.
The rest of this paper is organized as follows. Section 2 presents a literature review and hypothesis development. Section 3 presents the research methodology adopted for measurement scale development, data collection, and data analysis. Section 4 presents the theoretical and practical implications of this study, discusses study limitations, and describes directions for future research.

2 Literature Review and Hypothesis Development

E-market consumers may be reluctant to provide personal information (e.g., name, email address, phone number) [38] to access free browser content [5]. Consumers may rely on governmental laws and regulations or institutional safeguards and policies to protect their privacy. This study determined that the perceived effectiveness of governmental regulations refers to people's belief that laws protect them from personal data misuse by online businesses; the perceived effectiveness of business privacy policies refers to people's belief that online businesses do not use consumers' personal information for purposes other than those stated on their websites.

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762019000200106

2.1 Effects of Perceived Effectiveness of Privacy Legislations on Perceived Effectiveness of Business Privacy Policies, Consumer Trust in Service Providers, and Perceived Privacy Risk

Perceived effectiveness of privacy legislations relates to the belief among consumers that e-commerce marketers would abide by relevant privacy laws and that such laws would protect consumers from opportunism from firms [61]. Consumers expect governmental regulations to manage the collection, storage, and usage of their personal information [16]. The legislation embodies the institutional structural assurances provided by governmental agencies and affects consumer privacy-related beliefs [61]. Perceived effectiveness of privacy policy refers to the belief among web consumers that websites' privacy notices are accurate and offer reliable information about a firm's practices in protecting consumer privacy [62]. Privacy advocates and consumers sometimes question the effectiveness of industry self-regulation in protecting consumer privacy; therefore, they request effective legislations to reduce firm abuse of consumers' personal information [16]. Because of coercion and the threat of government sanctions, governmental regulations and laws often guide organizational actions and perspectives [42]. Additionally, because consumers recognize the powerful mechanisms of legal systems, they tend to believe that service providers would abide by the law [61]. A higher perceived effectiveness of privacy legislations indicates a higher likelihood of it being associated with perceived effectiveness of business privacy policies. Therefore, this paper proposes Hypothesis 1.

H1: Perceived effectiveness of privacy legislations positively influences perceived effectiveness of business privacy policies.

Trust is defined as a psychological state characterized by the extent to which a person is willing to believe that others are essentially honest [23] and his or her tendency to rely on others [62]. A previous study indicated that a buyer's trust in a seller in e-commerce plays a critical role in purchase decisions [31]. Perceived effectiveness of relevant privacy legislations refers to the likelihood of consumers believing that the legal assurance of their privacy rights protects them from firms misusing their personal information [61], which relates to the likelihood of them trusting e-commerce firms. Studies have suggested that progress toward specific security or privacy objectives might engender consumer trust [25]. Therefore, this paper proposes Hypothesis 2:

H2: Perceived effectiveness of privacy legislations positively influences trust in service providers.

Providing online firms with personal information may lead to consumers perceiving unexpected problems or fearing how their personal information might be used [29]. Consumers aware of privacy legislations tend to believe that the service providers would use their personal information appropriately after collection and that the legal assurance of their privacy rights should safeguard them from potential harm [61], which would in turn reduce their privacy risk concerns. Thus, this paper proposes Hypothesis 3:

H3: Perceived effectiveness of privacy legislations negatively influences perceived privacy risk.

2.2 Effects of Online Business Brand Image on Trust in Service Providers and Perceived Benefits of Information Disclosure

Walczak and Gregg [57] indicated that consumers' trust and beliefs in e-businesses are formed by their mental images of e-businesses. Brand image refers to consumer perceptions toward a particular brand and brand association through memory [53]. A study proposed that brand image contributes to the formation of consumer trust in vendors [11], and Esch et al. [18] further confirmed the brand image-brand trust relationship. Because brand image formed by consumers' prior knowledge and experiences, thereby cultivating their brand evaluations, previous studies have indicated that brand image affects consumer trust in specific brands [34], [55], [66]. Therefore, according to relevant studies, this paper proposes Hypothesis 4:

H4: Online business brand image positively influences trust in service providers.

Studies have defined brand image as sets of brand associations held by consumers [37], [58]. A previous study indicated that a favorable brand image leads to a positive halo effect and positively influences other brand associations [27]. The halo effect refers to a bias in which the overall impressions of specific traits of a subject under evaluation serve as a basis for evaluating other traits of said subject [46]. When a firm's brand image is favorable, proactive firm activities are perceived more positively by consumers [27]. Brand image relates to the favorability, strength, and uniqueness associated with a brand [3] including product-related and non-product-related attributes and benefits [13]. Consumer-perceived benefits are consumers' perceptions of product benefits [8]. Thus, brand image refers to consumers' perceptions of a brand based on the perceived benefits of the products or services offered by the brand [12]. Therefore, this paper proposes Hypothesis 5:

H5: Online business brand image positively influences perceived benefits of information disclosure.

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762019000200106

2.3 Effects of Trust in Service Providers on Perceived Effectiveness of Business Privacy Policies, Perceived Benefits of Information Disclosure, and Perceived Privacy Risk

Trust refers to the extent to which people have confidence in a party's goodwill and capacity to keep its promises, thereby influencing the perceived regularity and predictability of outcomes of exchanges with said party [4]. Perceived effectiveness of business privacy policies refer to the extent to which people believe that firms' privacy policies posted online provide accurate and reliable information about their privacy practices [62]. Generally, if a consumer lacks trust in a service provider, he or she perceives the provider's privacy policy to be less effective. In other words, perceived effectiveness of firm privacy policies is higher among individuals with more confidence in a firm's goodwill. Therefore, this paper proposes Hypothesis 6:

H6: Trust in service providers positively influences perceived effectiveness of business privacy policies.

Cooperative behaviors, such as sharing potentially sensitive information with other parties, are only possible if one party trusts the other party [9]. Researchers have identified that trust in service organizations affects users' data disclosure behavior [52]. A previous study indicated that trust in a party yields a higher likelihood of assessing the performance of the party favorably [14]. People who trust service providers believe that service providers have the ability to offer a positive utility, thereby enhancing the perceived usefulness of the provided service [71]. Therefore, an individual with greater trust in a firm has a higher expectation of the benefits of disclosing personal information online. Therefore, this paper proposes Hypothesis 7:

H7: Trust in service providers positively influences perceived benefits of information disclosure.

Trust enables online consumers to believe that web service providers collect, store, and use their privacy information appropriately, thereby reducing their concerns regarding personal information disclosure. A previous study suggested that a higher level of trust in a party's competence, reliability, and capability to safeguard personal information is associated with a lower degree of perceived privacy risk [15]. In addition, studies have proposed that trust in technology service providers can reduce consumer perceptions of risk [39], [68], and one study determined the effects of trust on perceived privacy risk [71]. Therefore, this paper proposes Hypothesis 8:

H8: Trust in service providers negatively influences perceived privacy risk.

2.4 Effects of Perceived Effectiveness of Business Privacy Policies on Perceived Privacy Risk

A study suggested that privacy protection may be a main value proposition in the online business market [44]. Perceived effectiveness of business privacy policies refers to the degree to which people believe that the institutional mechanisms established by businesses for protecting personal information are reliable. A previous study suggested that firms' initiative of informing consumers of their privacy practices leads to lower risk perceptions toward personal information disclosure [62]. Therefore, this paper proposes Hypothesis 9:

H9: The perceived effectiveness of business privacy policies negatively influences perceived privacy risk.

2.5 Effects of Perceived Benefits of Information Disclosure on Perceived Privacy Risk

Perceived benefits of information disclosure refer to the overall positive utility of using a particular website after disclosing personal information [43]. The benefits offered by service providers in exchange for information disclosure may alleviate risk perceptions. Studies have suggested that people who perceive the potential for achieving a positive net outcome (i.e., the benefits exceed the cost of disclosure) are more likely to accept the potential risks associated with disclosing personal information [16]. One previous study proposed that perceived benefits of information disclosure reduce individuals' intentions to protect themselves from risk [65]. The greater the perceived benefits of information disclosure, the lower the risk perception. Dinev et al. [16] found that perceived benefits of information disclosure negatively affect consumer perceptions of privacy risk. Therefore, this paper proposes Hypothesis 10:

H10: The effect of perceived benefits of information disclosure negatively influences perceived privacy risk.

The constructs and associations discussed in this section are presented graphically in Figure 1.

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 14 / ISSUE 2 / MAY 2019 / 59-69

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762019000200106

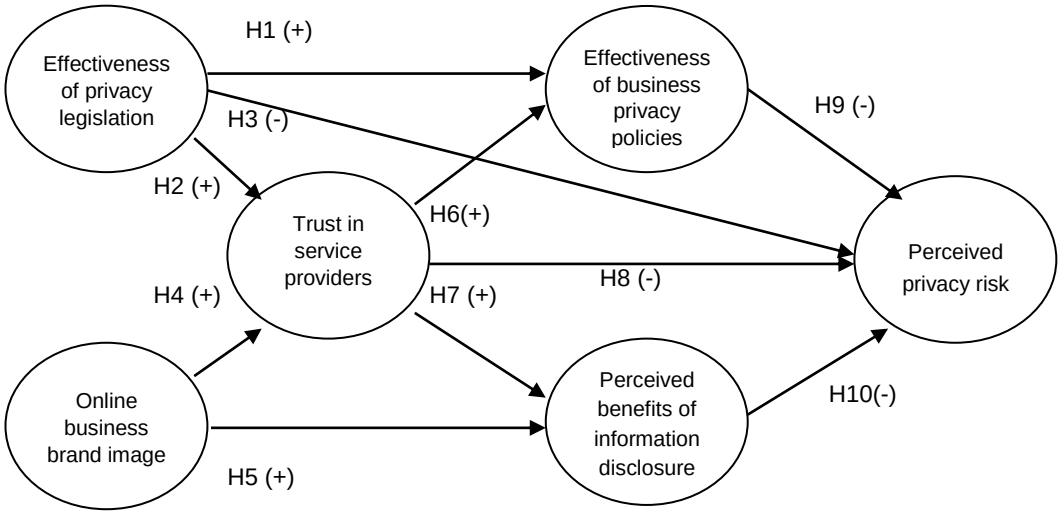

Figure 1: Theoretical research framework

3 Research Methodology

This section gives an outline of research methods that were followed in the study. It provides information on the research scale and instrument that was used for questionnaire design and data collection. Lastly, the methods used to analyze the data are also described.

3.1 Scale Development

Research scales were developed according to the relevant literature. The measurement scales for the perceived effectiveness of privacy legislation and the perceived effectiveness of business privacy policies were modified from 2 three-item scales obtained from the study of Xu et al. [62]. Online business brand image was measured using a three-item scale modified from the study of Yang and Ha [64]. Trust in online service providers and perceived privacy risk were measured using six- and five-item scales developed by Krasnova et al. [39], respectively. Finally, perceived benefits of information disclosure were assessed using a three-item scale derived from the study of Dinev et al. [16]. In summary, the questionnaire comprised 23 questions for testing the 10 hypotheses shown in Figure 1. A complete list of the six latent factors with the 23 items measured (including full statements) is show in Table 1. In addition, a 7-point Likert scale was employed for all measurements.

3.2 Sample and Data Collection

Data were collected from university campuses in Taiwan through surveys issued to students. Potential participants were approached individually and asked to participate in an academic study on personal information disclosure behavior. A filter question (i.e., *Have you provided accurate personal information to online service providers within the past 3 months?*) was asked to those who agreed to participate in order to exclude participants not belonging to the target sample. Respondents belonging to the target sample were issued a two-page questionnaire, and they were subsequently requested to provide answers based on the online service provider to which they had most recently disclosed personal information. Although no incentives were offered, of the 746 students from whom participation was requested, 425 voluntarily participated in this study (57% response rate). This study employed a self-completed survey method to ask the participants about their perceptions toward the research constructs. All constructs were measured using multi-item scales validated in previous studies. The respondents' demographic information (gender and age) and types of disclosed information were collected. Regarding demographics, 130 participants were men (30.7%) and 295 were women (69.3%). Most of the participants were aged 20-29 years (60.9%). Regarding information disclosure types, 92% of the participants reported their names, 87% reported email addresses, 82% reported gender, 76% reported phone numbers, 47% reported physical addresses, and 8% reported credit card information.

3.3 Data Analysis

This study employed LISREL 8.7 to validate the measurement model and test the hypotheses in the hypothesized structural models. Confirmatory factor analysis was initially used to assess the validity and reliability of each construct by using the average variance extracted (AVE) and composite reliability (CR) values. The analysis results

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 14 / ISSUE 2 / MAY 2019 / 59-69

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762019000200106

are shown in Table 1. All scale CR values were within 0.83-0.91, thereby exceeding the acceptance threshold of 0.70 [24]. Moreover, to assess discriminant validity, the Fornell-Larcker test [19] was performed. Table 2 shows that each construct achieved discriminant validity, all having AVE values greater than the squared correlations between pairs of latent variables, indicating discriminant validity is demonstrated [32].

Table 1: Accuracy analysis statistics

Research Constructs	Measurement Items	Factor Loading (λ)	Theta (*θ*)	C.R	AVE
Perceived effectiveness of privacy legislations	I feel confident that privacy protection laws reflect their commitments to protect my personal information.	0.76	043	0.82	0.60
	With the privacy protection laws, I believe that my personal information will be kept private and confidential by the Web site.	0.83	0.31		
	I believe that the privacy protection laws are an effective way to protect my personal information	0.73	0.46		
Perceived effectiveness of privacy policy	I feel confident that the Web site's privacy statements reflect their commitments to protect my personal information.	0.84	0.29	0.89	0.73
	With their privacy statements, I believe that my personal information will be kept private and confidential by the Web site.	0.91	0.17		
	I believe that the Web site's privacy statements are an effective way to demonstrate their commitments to privacy.	0.81	0.34		
Online business brand image	I have always had a good impression of this Web site.	0.86	0.27	0.88	0.72
	In my opinion, this Web site has a good image in the minds of consumers.	0.89	0.20		
	I believe that this the Web site has a better image than its competitors.	0.79	0.38		
Trust in service providers	The Web site is open and receptive to the needs of its members	0.73	0.46	0.91	0.63
	The Web site makes good-faith efforts to address most member concerns	0.77	0.40		
	The Web site is also interested in the well-being of its members, not just its own	0.77	0.41		
	The Web site is honest in its dealings with me	0.84	0.30		
	The Web site keeps its commitments to its members	0.82	0.33		
	The Web site is trustworthy	0.81	0.35		
Perceived benefits of information disclosure	Revealing my personal information on the Web site will help me obtain information/products/services I want.	0.88	0.23	0.88	0.72
	I need to provide my personal information so I can get exactly what I want from these Web sites.	0.92	0.15		
	I believe that as a result of my personal information disclosure, I will benefit from a better, customized service and/or better information and products.	0.73	0.47		
Perceived privacy risk	Overall, I see real threat to my privacy due to my presence on the Web site.	0.67	0.55	0.83	0.50
	I fear that something unpleasant can happen to me due to my presence on the Web site.	065	0.57		
	I feel risky publishing my personal information on the Web site.	0.87	0.25		
	Overall, I find it risky to publish my personal information on the Web site.	0.58	0.67		
	Overall, the perceived privacy risk involved when using the Web site is very risky	0.74	0.45		

Composite reliability: $CR = (\Sigma\lambda)^2/[(\Sigma\lambda)^2+\Sigma(\theta)]$
Average Variance Extracted: $AVE = (\Sigma\lambda^2)/[(\Sigma\lambda^2)+\Sigma(\theta)]$ (1)

Table 2: Correlation between research constructs

Research Constructs	Mean	S.D.		PEPL	PEPP	BBI	TSP	PBID	PPR
Perceived effectiveness of privacy legislations (PEPL)	4.10	1.04		**0.77**					
Perceived effectiveness of privacy policy (PEPP)	4.28	1.07		0.53	**0.86**				
Online business brand image (BBI)	4.82	0.93		0.35	0.48	**0.85**			
Trust in service providers (TSP)	4.68	0.86		0.43	0.63	0.56	**0.79**		
Perceived benefits of information disclosure (PBID)	4.56	0.95		0.44	0.61	0.46	0.60	**0.85**	
Perceived cyber privacy risk (PCPR)	3.70	0.98		0.42	0.56	0.28	0.41	0.48	**0.71**

Note: The square root of average variance extracted (AVE) for each construct (on the diagonal)
Scores: 1 - Strongly Disagree; 4 - Neutral; 7 - Strongly Agree

Model appropriateness was examined using fit indices. Structural model fit was assessed using the chi-square/df ratio, root mean square error of approximation (RMSEA), comparative fit index (CFI), nonnormed fit index (NNFI), incremental fit index (IFI), goodness-of-fit index (GFI), and adjusted goodness-of-fit index (AGFI). The structural model achieved favorable fit levels: chi-square/df = 2.99; RMSEA = 0.069; CFI = 0.98; NNFI = 0.97, IFI = 0.98; GFI =

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762019000200106

0.88; AGFI = 0.85. Because only a model with a GFI of <0.8 and RMSEA of >0.1 should be rejected [47], the model in this study satisfied the requirements. Regarding the framework of the current study, complete standardized path coefficients and *t* values were analyzed to determine whether the hypotheses were supported. Table 3 shows that H1, H2, H5, H6, H7, H9, and H10 were supported at a significance level of $p < 0.001$. Furthermore, H3 and H4 were supported at significance levels of $p < 0.01$ and $p < 0.05$, respectively. By contrast, H8 was not supported ($p > 0.05$). In addition, the explained variances obtained by predicting the constructs were 59% for perceived effectiveness of business privacy, 47% for trust in service providers, 43% for perceived benefits of information disclosure, and 43% for perceived privacy risk.

Table 3: Testing of the proposed hypotheses

	Path between	Path coefficients	t values
H1	Perceived effectiveness of privacy legislations→ Perceived effectiveness of privacy policy	＋0.35***	6.78
H2	Perceived effectiveness of privacy legislations →Trust in service providers	＋0.31***	5.92
H3	Perceived effectiveness of privacy legislations →Perceived privacy risk	-0.18**	2.66
H4	Online business brand image →Trust in service providers	＋0.13*	2.20
H5	Online business brand image →Perceived benefits of information disclosure	＋0.50***	9.14
H6	Trust in service providers →Perceived effectiveness of privacy policy	＋0.53***	9.68
H7	Trust in service providers →Perceived benefits of information disclosure	＋0.56***	8.56
H8	Trust in service providers →Perceived privacy risk	-0.06 ns	0.74
H9	Perceived effectiveness of privacy policy →Perceived privacy risk	-0.43***	5.09
H10	Perceived benefits of information disclosure →Perceived privacy risk	-0.24***	3.70

***: p-value < 0.001, **: p-value < 0.01, *: p-value < 0.05, ns: Not significant

To verify research results indicating that the perceived effectiveness of privacy policies and the benefits of information disclosure mediate the relationship between trust in service providers and privacy risk perceptions, the present study tested an alternative model in which perceived privacy risk mediated the relationship between perceived benefits and trust. This model was based on the findings of Catoiu et al. [10]; they observed that the relationship between perceived benefits and trust was mediated by perceived risk. The alternative model consisted of the hypothesized model but changed the direction of the two paths. The alternative model suggested that perceived benefits exert direct and indirect (through perceived privacy risk) effects on a user's perceived trust. To compare the two models, the Akaike information criterion (AIC) and the consistent Akaike information criterion (CAIC) were employed. Researchers have suggested that smaller values of these criteria indicate a better model fit [26]. The results revealed that for the hypothesized model, the AIC was 769.92 and the CAIC was 1056.23; for the alternative model, the AIC was 792.17 and the CAIC was 1078.78, indicating that the hypothesized model was superior to the alternative model.

4 Discussion

The results suggest that perceived effectiveness of privacy legislations and online business brand image affect people's trust in service providers. Trust in service providers enhances perceived effectiveness of business privacy policies and perceived benefits of information disclosure, which in turn negatively influence privacy risk perceptions. In addition, perceived effectiveness of privacy legislations positively influences perceived effectiveness of business privacy policies but negatively influences privacy risk perceptions. Online business brand image positively influences perceived benefits of information disclosure. In other words, people who perceive privacy legislations as more effective and brand image as more positive have higher trust in service providers, which in turn enhances their confidence in the effectiveness of service providers' privacy policies and services provided. Higher perceived effectiveness of business privacy policies and perceived benefits of information disclosure engender lower perceived privacy risk. Finally, a more positive brand image increases people's beliefs in the benefits provided by the brand. People who perceive higher effectiveness of privacy legislations also perceive higher effectiveness of business privacy policies and lower information disclosure risk.

4.1 Theoretical and Practical Implications

The present study found that perceived effectiveness of business privacy policies and perceived benefits of information disclosure negatively influence consumer perceptions toward privacy risk. These findings are consistent with those of Xu et al. [62] and Dinev et al. [16]. According to a literature review, no previous studies have focused on whether and how governmental laws and brand image affect privacy risk perceptions. Furthermore, whereas numerous studies have focused on the direct effects of various antecedent variables on privacy risk perceptions, little attention has been devoted to clarifying the underlying mechanisms of the relationship between the antecedent variables. Therefore, this paper contributes to the literature by providing results of an empirical test of a model designed to address how governmental privacy laws and online business brand image affect consumer trust in

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762019000200106

online businesses, perceived effectiveness of firm privacy policies, perceived benefits of information disclosure, and perceived privacy risk. Notably, no significant relationship was detected between consumer trust in online service providers and consumer-perceived privacy risk; this finding is inconsistent with those of previous research that indicated a negative effect of trust on perceived privacy risk [71].

Although this finding is unexpected, according to the research framework, the reason for the finding may be that trust may not always reduce the perception of risk if a firm's performance (i.e., effectiveness of its privacy policy and benefits of information disclosure) is perceived to be questionable and worthless. This implies that trust may not always reduce consumers' risk perceptions if their trust does not lead to they believe that a service provider's privacy policies are effective and whether they believe that information disclosure behavior will benefit from more effective, customized service and/or exceptional information and products. The results imply that the perceived effectiveness of privacy policies and the perceived benefits of information disclosure completely mediate the relationship between trust in service providers and privacy risk perceptions. Therefore, this study extends the literature by proposing integrative models for examining the hierarchical influences among these factors. Furthermore, the current study clarifies that governmental privacy laws indirectly (through trust in online businesses and effectiveness of firm privacy policies) and directly affect privacy risk perceptions. However, online business brand image indirectly affects consumer-perceived privacy risk through trust in online business and perceived benefits of information disclosure.

The voluntary disclosure of personal information plays a vital role in the success of e-commerce. However, privacy perceptions are associated with interactive processes. Online businesses must respond to the challenge of increased consumer privacy concerns by elucidating the mechanism for reducing online consumers' privacy risk perceptions. The findings of this study provide an understanding of the factors affecting privacy risk perceptions from the perspectives of government and firm performance. These findings serve as a reference for governments and firm administrators to understand how government and online business performance can reduce consumers' privacy risk perceptions. This study demonstrated that the perceived effectiveness of privacy legislation and online brand image are antecedents to trust in service providers, which in turn affect consumer-perceived effectiveness of privacy policies and the perceived benefits of information disclosure, which consequently negatively influence privacy risk perceptions. Based on these findings, this study offers numerous practical suggestions for reducing privacy risk perceptions from the perspectives of government and firm performance. First, the findings revealed that consumer-perceived effectiveness of governmental privacy legislation directly and indirectly (through the perceived effectiveness of privacy policies) affect their privacy risk perceptions. Thus, to manage privacy risk effectively, governments should focus on building consumers confidence in privacy protection laws by developing and maintaining an effective system of communication. Moreover, governments should ensure that laws are executed in the order they are listed in the laws pane to build consumer confidence in the laws as being an effective way to protect their personal information and to assure consumers that their personal information will be kept private and confidential by a website. Second, the results revealed that a positive online brand image increases consumer-perceived benefits of information disclosure, which results in lower privacy risk perceptions. That is, consumers with positive impressions of online businesses are more likely to believe that they will benefit from more effective, customized service and/or exceptional information and products, which reinforces their privacy risk perceptions. Thus, to increase consumer-perceived benefits of an online service and further reduce their privacy risk perceptions, online business should focus on creating a positive brand image by using promotional tools, such as an advertising strategy, to link favorable and positive associations to the brand in consumers' minds. Third, more trust in online service providers will increase consumer-perceived effectiveness of business privacy policies and the perceived benefits of information disclosure and in turn reduce their privacy risk perceptions. Thus, online service providers should focus on building consumer trust by being open and receptive to the needs of their members through making efforts to address their members' concerns, by being interested in the well-being of their members, by being committed to their members, and by being honest in their dealings with them. Finally, trust in service providers is affected by consumer-perceived effectiveness of privacy legislation and online brand image. Therefore, governments and online businesses should apply the findings to consider the role of privacy legislation and brand image and their effects on consumer trust in service providers.

4.2 Limitations, and Directions for Further Research

Although e-commerce has developed rapidly in recent years, the collection of consumer data to facilitate the exchange process and meet consumer needs remains critical for online businesses. The findings of this study could facilitate online businesses in developing effective programs for collecting consumer information from the perspectives of privacy legislations and firm brand image. However, despite its contributions, the present study has limitations. The first and one of the major limitations is the bias engendered by the younger (60.9% of the participants were aged 20-29 years) and female- dominated (69.3%) sample. In addition, the demographic groups in this study were not well defined. Future studies should replicate the study with participants of varying ages and with a greater balance between genders; testing the model on a sample of consumers of varying ages and with a greater balance between genders could provide less biased results. Second, a previous study applied the Big Five personality traits (agreeableness, conscientiousness, emotional stability, extroversion, and openness) to understand their effects on concern for privacy (CFP); the researchers' findings indicated that agreeableness is negatively associated with CFP in relation to location-based services, whereas conscientiousness and openness are positively associated with CFP [33]. Additional studies should include personality traits in the proposed model. An investigation of the moderating role of personality traits in the relationship between governmental (privacy legislation) and firm-related (online brand

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762019000200106

image) factors and consumer perceptions of online privacy risk will be useful for comparing personality traits. Third, the effects of social influence on individual perceptions have been documented in the literature [56], [67]. A social influencer refers to an individual who, through a close relationship with another person, has substantial influence on that person's technological perceptions [30]. Therefore, future studies could introduce social influence as an antecedent variable in the adopted research framework. In summary, by investigating the moderating roles of individual characteristics within the research frameworks and antecedent variables of the research construct factors, future studies are expected to provide more guidelines for research on consumer privacy risk as well as for practitioners.

5 Conclusion

With an increasing number of consumers using e-commerce platforms and the increasing importance of online markets, it is imperative for online marketers to develop a thorough understanding of effective approaches that reduce consumers' privacy risk perceptions. This study examined the effects of privacy legislation and online brand image factors on consumer perceptions of online privacy risk. A conceptual model was proposed to explore the underlying mechanisms of the effects of privacy legislation and online brand image on consumers' perceptions of online privacy risk, and the relationships among the perceived effectiveness of privacy legislation, brand image, trust in online businesses, the perceived effectiveness of privacy policies, the perceived benefits of information disclosure, and perceived privacy risk were hypothesized and examined. As predicted, the perceived effectiveness of privacy legislation, the perceived effectiveness of privacy policies, and the perceived benefits of information disclosure directly and negatively influenced perceived privacy risk. In contrast to previous studies, in the current study, trust in online businesses was not correlated with perceived privacy risk. Additionally, as expected, consumer-perceived effectiveness of privacy legislation and brand image positively influenced trust in online businesses, which consequently increased the perceived effectiveness of privacy policies and the perceived benefits of information disclosure, resulting in lower perceived privacy risk. The current study also investigated the impact of the perceived effectiveness of privacy legislation on the perceived effectiveness of privacy policies and the impact of brand image on the perceived benefits of information disclosure. Positive relationships were found. This research contributes by adding to our understanding of how and why privacy legislation and online brand image affect consumers' privacy risk perceptions.

References

[1] M. Adams, Big data and individual privacy in the age of the internet of things, Technology Innovation Management Review, vol. 7, no. 4, pp. 12-24, 2017.
[2] S. Agarwal and R. K. Teas, Perceived value: Mediating role of perceived risk, Journal of Marketing Theory and Practice, vol. 9, no. 4, pp. 1-14, 2001.
[3] A. Alamro and J. Rowley, Antecedents of brand preference for mobile telecommunications services, The Journal of Product and Brand Management, vol. 20, no. 6, pp. 475-486, 2011.
[4] P. Aurier and d. L. Gilles Séré, Impacts of in-store manufacturer brand expression on perceived value, relationship quality and attitudinal loyalty, International Journal of Retail & Distribution Management, vol. 39, no. 11, pp. 810-835, 2011.
[5] S. Bandyopadhyay, Online privacy concerns of Indian consumers, The International Business & Economics Research Journal, vol. 10, no. 2, pp. 93-100, 2011.
[6] S. Bandyopadhyay, Predicting consumer reaction to online privacy concerns: A nested logit model, International Journal of Management & Information Systems, vol. 17, no. 2, pp. 89-96, 2013.
[7] G. Bansal, F. M. Zahedi and D. Gefen, The role of privacy assurance mechanisms in building trust and the moderating role of privacy concern, European Journal of Information Systems, vol. 24, no. 6, pp. 624-644, 2015.
[8] X. Bian and L. Moutinho, The role of brand image, product involvement, and knowledge in explaining consumer purchase behaviour of counterfeits, European Journal of Marketing, vol. 45, no. 1, pp. 191-216, 2011.
[9] K. Boehm, S. Etalle, J. den Hartog, C. Huetter, S. Trabelsi, D. Trivellato, and N. Zannone, A flexible architecture for privacy-aware trust management, Journal of Theoretical and Applied Electronic Commerce Research, vol. 5, no. 2, pp. 77-96, 2010.
[10] Catoiu, M. Orzan, O. Macovei, and C. Iconaru, Modelling users' trust in online social networks, Amfiteatru Economic, vol. 16, no. 35, pp. 289-302, 2014.
[11] Y.-T. Chen and T.-Y. Chou, Exploring the continuance intentions of consumers for B2C online shopping, Online Information Review, vol. 36, no. 1, pp. 104-125, 2012.
[12] B. Chitty, S. Ward and C. Chua, An application of the ECSI model as a predictor of satisfaction and loyalty for backpacker hostels, Marketing Intelligence & Planning, vol. 25, no. 6, pp. 563-580, 2007.
[13] K. Chiu, R. Lin, M. K. Hsu, and L. Huang, Power of branding on internet service providers, The Journal of Computer Information Systems, vlo. 50, no. 3, pp. 112-120, 2010.
[14] P. L. Dawes and G. R. Massey, A study of relationship effectiveness between marketing and sales managers in business markets, The Journal of Business & Industrial Marketing, vol. 21, no. 6, pp. 346-360, 2006.
[15] T. Dinev and P. Hart, An extended privacy calculus model for E-commerce transactions, Information Systems Research, vol. 17, no. 1, pp. 61-80,100, 2016.

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762019000200106

[16] T. Dinev, H. Xu, J. H. Smith, and P. Hart, 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, 2013.
[17] M. Dupuis, S. Khadeer and J. Huang, I got the job!: An exploratory study examining the psychological factors related to status updates on facebook, Computers in Human Behavior, vol. 73, pp. 132-140, 2017.
[18] F.-R. Esch, T. Langner, B. H. Schmitt, and P. Geus, Are brands forever? how brand knowledge and relationships affect current and future purchases, The Journal of Product and Brand Management, vol. 15, no. 2, pp. 98-105, 2006.
[19] C. Fornell and D. F. Larcker, Evaluating structural equation models with unobservable variables and measurement error, Journal of Marketing Research, vol. 18, no. 1, pp. 39-50, 1981.
[20] T. J. Gerpott and S. Berg, Determinants of the willingness to use mobile location-based services, Business & Information Systems Engineering, vol. 3, no. 5, pp. 279-287, 2011.
[21] A. N. Giovanis, S. Binioris and G. Polychronopoulos, An extension of TAM model with IDT and security/privacy risk in the adoption of internet banking services in Greece, EuroMed Journal of Business, vol. 7, no. 1, pp. 24-53, 2012.
[22] S. Godoy, C. Labarca, N. Somma, M. Gálvez, and M. Sepúlveda, Circumventing communication blindspots and trust gaps in technologically-mediated corporate relationships: The case of Chilean business-to-consumer E-commerce, Journal of Theoretical and Applied Electronic Commerce Research, vol. 10, no. 2, pp. 19-32, 2015.
[23] L. Gwebu, J. Wang and M. D. Troutt, A conceptual framework for understanding trust building and maintenance in virtual organizations, Journal of Information Technology Theory and Application, vol. 9, no. 1, pp. 43-63, 2007.
[24] J. Hair, W. C. Black, B. J. Babin, R. E. Anderson, and R. Tatham, Multivariate Data Analysis. Upper Saddle River, N.J: Pearson Prentice Hall, 2006.
[25] S. Y. Hashemi and S. H. Parisa, Security, privacy and trust challenges in cloud computing and solutions, International Journal of Computer Network and Information Security, vol. 6, no. 8, pp. 34-40, 2014.
[26] T. Hennig-Thurau, K. P. Gwinner and D. D. Gremler, Understanding relationship marketing outcomes: An integration of relational benefits and relationship qualityl Journal of Service Research, vol. 4, no. 3, pp. 230-247, 2002.
[27] A.-T. Hsieh and C.-K. Li, The moderating effect of brand image on public relations perception and customer loyalty, Marketing Intelligence & Planning, vol. 26, no. 1, pp. 26-42, 2008.
[28] C. Hsu and J. C. Lin, Exploring factors affecting the adoption of internet of things services, The Journal of Computer Information Systems, vol. 58, no. 1, pp. 49-57, 2018.
[29] H. Im and Y. Ha, Is this mobile coupon worth my private information?, Journal of Research in Interactive Marketing, vol. 9, no. 2, pp. 92-109, 2015.
[30] J. Jarvelainen, Online purchase intentions: An empirical testing of a multiple-theory model, Journal of Organizational Computing and Electronic Commerce, vol. 17, no. 1, pp. 53-74, 2007.
[31] J. Joo, Roles of the buyer's trust in seller in posted-price model of consumer to consumer E-commerce, Journal of Theoretical and Applied Electronic Commerce Research, vol. 10, no. 3, pp. 30-44, 2015.
[32] J. M. Jung, K. Polyorat and J. J. Kellaris, A cultural paradox in authority-based advertising, International Marketing Review, vol. 26, no. 6, pp. 601-632, 2009.
[33] A. Junglas, N. A. Johnson and C. Spitzmüller, Personality traits and concern for privacy: An empirical study in the context of location-based services, European Journal of Information Systems, vol. 17, no. 4, pp. 387-402, 2008.
[34] D. Ke, A. Chen and C. Su, Online trust-building mechanisms for existing brands: The moderating role of the e-business platform certification system, Electronic Commerce Research, vol. 16, no. 2, pp. 189-216, 2016
[35] J. Keith, J. S. Babb, P. B. Lowry, C. P. Furner, and A. Abdullat,
[36] E. Kemp and M. Bui, Healthy brands: Establishing brand credibility, commitment and connection among consumers, The Journal of Consumer Marketing, vol. 28, no. 6, pp. 429-437, 2011.
[37] W. G. Kim and H.-B. Kim, Measuring customer-based restaurant brand equity: Investigating the relationship between brand equity and firms performance, Cornell Hospitality Quarterly, vol. 45, no. 2, pp. 115-131, 2004.
[38] A. Kolsaker and C. Payne, Engendering trust in e-commerce: A study of gender-based concerns, Marketing Intelligence & Planning, vol. 20, no. 4, pp. 206-214, 2002
[39] H. Krasnova, S. Spiekermann, K. Koroleva, and T. Hildebrand, Online social networks: Why we disclose, Journal of Information Technology, vol. 25, no. 2, pp. 109-125, 2010.
[40] Y. Le, T. Zhang, X. Luo, L. Xue, and H. Chang, Toward automatically generating privacy policy for android apps, IEEE Transactions on Information Forensics and Security, vol. 12, no. 4, pp. 865-880, 2017.
[41] H. Li, R. Sarathy and H. Xu, Understanding situational online information disclosure as a privacy calculus, The Journal of Computer Information Systems, vol. 51, no. 1, pp. 62-71,2010.
[42] J. Li, J. Moy, K. Lam, and C. W. Chu, Institutional pillars and corruption at the societal level, Journal of Business Ethics, vol. 83, no. 2, pp. 327-339, 2008.
[43] Y. Li and X. Wang, Online social networking sites continuance intention: A model comparison approach, The Journal of Computer Information Systems, vol. 57, no. 2, pp. 160-168, 2017.
[44] Z. Liu, R. Bonazzi, B. Fritscher, and Y. Pigneur, Privacy-friendly business models for location-based mobile services, Journal of Theoretical and Applied Electronic Commerce Research, vol. 6, no. 2, pp. 90-107, 2011.
[45] C. G. Mieres, A. M. D. Martín and J. A. T. Gutiérrez, Influence of perceived risk on store brand proneness, International Journal of Retail & Distribution Management, vol. 34, no. 10, pp. 761 -772, 2006.

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762019000200106

[46] B. Muhammad and M. Aftab, Incorporating attitude towards halal banking in an integrated service quality, satisfaction, trust and loyalty model in online Islamic banking context, The International Journal of Bank Marketing, vol. 31, no. 1, pp. 6-23, 2013.
[47] A. Mukherjee and N. Malhotra, Does role clarity explain employee-perceived service quality?, International Journal of Service Industry Management, vol. 17, no. 5, pp. 444-473, 2006.
[48] P. O'Connor, What happens to my information if I make a hotel booking online: An analysis of on-line privacy policy use, content and compliance by the international hotel companies, Journal of Services Research, vol. 3, no. 2, pp. 5-28, 2004.
[49] O. F. Ogunlana, I. A. O. Bakare and O. A. Omobitan, Government spending, corruption and output growth in Nigeria, Arabian Journal of Business and Management Review, vol. 5, no. 10, pp. 55-71, 2016.
[50] S. Okazaki, H. Li and M. Hirose, Consumer privacy concerns and preference for degree of regulatory control: A study of mobile advertising in Japan, Journal of Advertising, vol. 38, no. 4, pp. 63-77, 2009.
[51] J. Ortiz, W. Chih and F. Tsai, Information privacy, consumer alienation, and lurking behavior in social networking sites, Computers in Human Behavior, vol. 80, pp. 143-157, 2018.
[52] A. Rohunen, J. Markkula, M. Heikkilä, and J. Heikkilä, Open traffic data for future service innovation - addressing the privacy challenges of driving data, Journal of Theoretical and Applied Electronic Commerce Research, vol. 9, no. 3, pp. 71-89, 2014.
[53] A. Sassenberg, Effects of sport celebrity transgressions: An exploratory study, Sport Marketing Quarterly, vol. 24, no. 2, pp. 78-90, 2015
[54] K. H. Smith, F. A. Méndez Mediavilla and G. L. White, The impact of online training on facebook privacy, The Journal of Computer Information Systems, vol. 58, no. 3, pp. 244-252, 2018.
[55] S. F. Syed Alwi, B. Nguyen, T. C. Melewar, Y. H. Loh, and M. Liu, Explicating industrial brand equity, Industrial Management & Data Systems, vol. 116, no. 5, pp. 858-882, 2016.
[56] E. E. Umphress, G. Labianca, D. J. Brass, E. Kass, and L. Scholten, The role of instrumental and expressive social ties in employees' perceptions of organizational justice, Organization Science, vol. 14, no. 6, pp. 738-753, 2003.
[57] S. Walczak and D. G. Gregg, Factors influencing corporate online identity: A new paradigm, Journal of Theoretical and Applied Electronic Commerce Research, vol. 4, no. 3, pp. 17-29, 2009.
[58] P. Z. Wang, C. Menictas and J. J. Louviere, Comparing structural equation models with discrete choice experiments for modelling brand equity and predicting brand choices, Australasian Marketing Journal, vol. 15, no. 2, pp. 12-25, 2007.
[59] J. Wirtz, M. O. Lwin and J. D. Williams, Causes and consequences of consumer online privacy concern, International Journal of Service Industry Management, vol. 18, no. 4, pp. 326-348, 2007.
[60] F. Xu, K. Michael and X. Chen, Factors affecting privacy disclosure on social network sites: An integrated model, Electronic Commerce Research, vol. 13, no. 2, pp. 151-168, 2013.
[61] H. Xu, Consumer responses to the introduction of privacy protection measures: An exploratory research framework, International Journal of E-Business Research, vol. 5, no. 2, pp. 21-47, 2009
[62] H. Xu, T. Dinev, J. Smith, and P. Hart, Information privacy concerns: Linking individual perceptions with institutional privacy assurances, Journal of the Association for Information Systems, vol. 12, no. 12, pp. 798-824, 2011.
[63] H. Yang, Young American consumers' prior negative experience of online disclosure, online privacy concerns, and privacy protection behavioral intent, Journal of Consumer Satisfaction, Dissatisfaction and Complaining Behavior, vol. 25, 179-202, 2012.
[64] S. Yang and S. Ha, Brand knowledge transfer via sponsorship in the financial services industry, The Journal of Services Marketing, vol. 28, no. 6, pp. 452-459, 2014.
[65] S. Youn, Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents, The Journal of Consumer Affairs, vol. 43, no. 3, pp. 389-418, 2009.
[66] S. Y. Yung and Y. Li, Building trust in m-commerce: Contributions from quality and satisfaction, Online Information Review, vol. 33, no. 6, pp. 1066-1086, 2009.
[67] T. J. Zagenczyk, R. Gibney, W. T. Few, and R. L. Purvis, The ties that influence: A social network analysis of prototypical employees' effects on job attitudes among coworkers, Journal of Management Policy and Practice, vol. 14, no. 4, pp. 26-42, 2013.
[68] T. Zhou, Examing location-based services usage from the perspectives of unified theory of acceptance and use of technology and privacy risk, Journal of Electronic Commerce Research, vol. 13, no. 2, pp. 135-144, 2012.
[69] T. Zhou, An empirical examination of user adoption of location-based services, Electronic Commerce Research, vol. 13, no. 1, pp. 25-39, 2013.
[70] T. Zhou, Examining continuous usage of location-based services from the perspective of perceived justice, Information Systems Frontiers, vol. 15, no. 1, pp. 141-150, 2013.
[71] T. Zhou, Understanding user adoption of location-based services from a dual perspective of enablers and inhibitors, Information Systems Frontiers, vol. 17, no. 2, pp. 413-422, 2015.