FACILITATING GLOBAL E-COMMERCE: A COMPARISON OF CONSUMERS' WILLINGNESS TO DISCLOSE PERSONAL INFORMATION ONLINE IN THE U.S. AND IN INDIA

Babita Gupta
California State University Monterey Bay
100 Campus Center, Seaside, CA 93955
bgupta@csumb.edu

Lakshmi S. Iyer
The University of North Carolina at Greensboro
479 Bryan Building, Greensboro, NC 27402
Lsiyer@uncg.edu

Robert S. Weisskirch
California State University Monterey Bay
100 Campus Center, Seaside, CA 93955
rweisskirch@csumb.edu

ABSTRACT

Consumers' privacy and security concerns are magnified as companies rely on worldwide networks for electronic commerce. Global businesses that can persuade consumers to disclose their personal information online are more likely to provide better service and product delivery. In this research, we conducted an empirical study of 809 consumers in the U.S. and India to investigate their online information disclosing behavior and their intentions to take and execute protective measures during online interactions. Results suggest that there are significant differences between American and Indian consumers with regards to their willingness to disclose personal information (WDPI), and their intentions and actions for privacy and security protection. We find that Indian consumers are more willing to disclose potentially sensitive personal information, and U.S. consumers intend to and engage in higher passive privacy protection actions compared to Indians. Thus, cultural differences influence consumers' WDPI and their online privacy protection behavior. These findings have implications for companies to consider cultural differences when conducting global e-commerce, indicating a need for a localization approach.

Keywords: online privacy, online security, information disclosure, online consumer behavior, cultural differences, U.S., India

1. Introduction

Across the globe, businesses and organizations rely on personal information disclosed by consumers during online transactions to develop strategies to enhance the online experience and maximize profitability. Companies that can influence their customers to disclose personal information online are likely to have greater opportunities to leverage the online channel to increase revenues. However, research indicates that issues such as privacy and security of networks and encryption policies influence adoption and success of e-commerce practices [Brown & Muchira, 2004; Painea, Reipsb, Stiegerc, Joinsona & Buchanan, 2007].

The degree of privacy sensitivity and privacy concerns for data protection of citizens may be rooted in cultural differences among nations [Pavlou and Chai, 2002; Rudraswamy and Vance, 2001]. Although there are studies in the U.S. that have investigated the willingness of consumers to disclose personal information online [Earp and Baumer, 2003; Son and Kim, 2008], there is little cross-cultural research that provides granular details on the types of personal information consumers are willing to disclose online and any differences across cultures [Meinert, Peterson, Criswell, and Crossland, 2006]. This study fills this gap in the literature by comparing consumers' willingness to disclose *different types* of personal information between two countries: the U.S. and India. In addition, given that privacy concerns continue to be a major barrier to e-commerce growth [Hann, Hui, Lee, and Png, 2007; Painea *et al.* 2007], this study empirically examines consumers' willingness to disclose personal

information (WDPI) with the protective measures they take and how these behaviors differ across two different cultures: Indian and American.

Examining these issues is important for two major reasons. First, global companies that better understand the differences in consumer intention and practices towards protecting privacy and security and consumers' willingness to disclose information are then likely to be poised for e-commerce growth by utilizing that information. Second, since U.S.-based and multinational companies have many outsourcing contracts with Indian companies, understanding the protective intentions and actions of Indian users regarding disclosing personal information is critical to sustaining business profitability. In a recent study, Kumaraguru, Cranor, and Newton [2005] found that Indians and Americans have differing levels of concerns about online privacy, and that the U.S. consumers are more aware of online privacy issues. However, their study did not explore specific differences between these two diverse groups of consumers with regards to personal information disclosure and consumers' protective intentions and actions. The current study explores these differences between cultures, so that companies can better understand consumers' WDPI online and actions they take to protect themselves. Organizations looking to expand e-commerce in either culture can formulate appropriate strategies and policies to collect personal information from consumers to provide customized services. We next present the theoretical foundations for development of the research hypotheses, followed by description of the research methodology, results and discussion of results, concluding with implications and directions for future research.

2. Theoretical Background

2.1. Information Privacy Concerns, Willingness to Disclose Personal Information (WDPI) Online, and Consumer's Protective Behavior.

In this study, we focus on the privacy concerns of consumers as measured by their WDPI during online interactions with firms. During online transactions, consumers may be asked to share demographic information, email address, credit card numbers, financial data, medical records, habits, preferences, or other personal information. Consumers may be wary of disclosing personal, identifying, and sensitive information, which is reflected in their willingness to disclose such information. This may be rooted in cultural perceptions. Studies, primarily about the U.S. consumers, have established that consumers have higher concerns about sharing sensitive personal information such as social security, health, medical and financial data [Lanier and Saini, 2008; Phelps, Nowak and Ferrell, 2000; Sheehan and Hoy 2000]. However, these studies did not consider cultural differences in the willingness to share specific personal information.

Online information privacy concerns arise when a consumer's personally identifiable information is either collected without a consumer's consent or is misused in a manner that is not consistent with FTC's fair information practices. Thus, a consumer's online privacy concerns reflect the potential vulnerability of their personal information provided online to a firm [Castañeda and Montoro, 2007; Hann *et al.*, 2007; Sheng, Nah, and Siau, 2008].

Studies show that consumers do not have sufficient awareness and understanding about online security issues and do not fully understand their role in protecting themselves online [Zhang, 2005]. Some consumers manage their online privacy concerns by reading the website's privacy and security policies, not disclosing personal information, providing false personal information, opting out of marketing communication options ("passive reaction"), using online anonymous software to hide their identity, or creating false identities [Gauzente, 2004; Lanier and Saini, 2008; Sheehan and Hoy, 2000].

Thus, consumers with higher privacy concerns would be less willing to disclose their personal information online, particularly sensitive information. In addition, increased privacy concerns lead to greater likelihood of a consumer providing incomplete or false information to web sites, being more proactive in opting out and being less likely to register with web sites requesting information. The Nam, Song, Lee, and Park [2006] study found that companies with privacy policies and third-party privacy seals clearly displayed on their websites were more likely to elicit accurate and current data from consumers. Studies have found a positive relationship between consumers' perceptions of a company's respect for consumer privacy (such as websites with strong privacy policies) and consumers' WDPI online to that company, thus affecting consumers' protective strategies like withholding sensitive information or refusing to purchase [Lauer and Deng, 2007; Lwin, Wirtz, and Williams, 2007].

2.2. Culture, Online Privacy, and Online Consumer Behavior

2.2.1. The U.S. and India: Cultural and Technological Differences

The U.S. and India differ in culture, technology infrastructure, use of information and communication technologies (ICTs), and internet adoption. Table 1 summarizes cultural comparison between the U.S. and India based on Hofstede's [1984, 2001] culture dimensions.

Table 1: The U.S. and India - Cultural Dimensions Comparison[1] [Hofstede, 2001]

Culture Dimension	United States	India
Power Distance	40	77
Individualism	91	48
Masculinity	62	56
Uncertainty Avoidance	46	40
Long Term Orientation	29	61

As a culture, India has a higher power distance index which indicates that Indians are more comfortable with centralized power than individuals from low power distance cultures such as American culture. A higher value for individualism implies that individuals from that culture view self and immediate family as relatively more important than communal groups, focusing on individual achievement over collective achievement. The U.S. is a slightly more masculine culture than India, emphasizing work and material accomplishments as relatively more important than human relationships. Lower index scores on uncertainty avoidance signifies that people prefer situations that are free and not bound by rules and regulations as compared to higher uncertainty avoidance. Cultures with higher long-term orientation follow traditions and value perseverance while short-term cultures focus on maintaining materialistic status. As noted above, in comparison to the United States, India, as a culture, is much higher on power distance, lower on individualism (i.e., greater on collectivism), slightly lower on masculinity and uncertainty avoidance, and higher on long term orientation.

Beyond the cultural differences, the United States and India vary in other technology dimensions. As of 2008, the U.S. had nearly 75% of its population using the Internet while India only had about 7% of its population using the Internet [Internet World Statistics, 2009]. The U.S. ranks as the third most networked economy in the world and India ranks 54th in networked readiness [The Global Information Technology Report, 2009]. However, the growth rate of the Internet users in India has been more than a 1005% from 2000 to 2008 [Internet World Statistics, 2009], which provides tremendous growth opportunities for global companies wishing to engage in e-commerce in India.

Similar disparities exist between the number of consumers who own credit cards in India and the U.S. Since credit cards are one of the primary modes of payment mechanisms for online transactions, and consumers are required to share personal information for such transactions, it is important to understand consumers' concerns and behaviors with regards to sharing of personal information online. As of 2007, India had 22 million credit card users [Schulz, 2008] while the U.S. had about 173 million credit card owners with one or more cards and 1.5 billion credit cards in use in 2006 [Woolsey and Schulz, 2009].

2.2.2. Role of Culture in Consumers' Information Disclosing and Protective Behavior

Culture of a particular country may influence the privacy concerns of its citizens and hence influence Internet use and online shopping rates [Bellman, Johnson, Kobrin, and Lohse, 2004; Lanier and Saini, 2008; Singh and Baack, 2004]. In comparing website preferences of consumers in countries in Asia (India and China) and Europe (Germany, Italy, Netherlands, Spain, and Switzerland), consumers preferred culturally-adapted, local web sites, and culture influenced consumer's beliefs, attitudes and intention to buy online [Singh, Fassott, Zhao and Boughton, 2006; Singh, Furrer and Ostinelli, 2004]. Fusilier and Durlabhji [2005] found that in less individualistic cultures such as India, social factors like social pressure and social expectations can be an important positive influence on Internet use and online behavior. Individuals from cultures high in individualism, masculinity, and uncertainty avoidance indices and low in power distance and long term orientation indices (such as the U.S.) have a higher comfort (or trust) with impersonal activities such as the online activities, than individuals from cultures exhibiting the opposite levels (such as India) [Gefen and Heart, 2006; Kivijärvi, Laukkanen and Cruz, 2007; Muthitacharoen and Palvia, 2002].

A consumer's willingness to trust that the provider will fulfill their perceived obligation in an appropriate manner is crucial to e-commerce [Gefen and Heart, 2006; Yoon, 2009]. Individualistic cultures tend to develop higher initial trust towards others more readily than do the less individualistic countries like India [Gefen and Heart, 2006; Van Slyke, Belanger and Sridhar, 2005]. This greater initial trust is developed because in individualistic cultures, people expect others to follow the accepted rules of conduct and, therefore, are more willing to rely on strangers [Gefen and Heart, 2006]. Thus, consumers in higher individualistic countries such as the U.S. are more willing to trust others outside the extended family [Gefen and Heart, 2006; Yoon, 2009]. Using the Internet is an impersonal activity compared to the more social activity such as conventional shopping in brick-and-mortar stores [Muthitacharoen and Palvia, 2002; Van Slyke *et al.*, 2005]. Therefore, in individualistic cultures such as the U.S.,

[1] www.geert-hofstede.com, Accessed on April 16, 2009

consumers should be more willing to engage in impersonal activities such as the online transactions, and be more willing to share their personal information with online vendors compared to the consumers from a collectivistic culture like India.

With regards to power distance index (PDI), empirical research has shown that consumers from higher PDI countries such as India are less likely to trust service providers and have higher privacy concerns than do the consumers from low PDI country such as the U.S. [Bellman *et al.* 2004; Gefen and Heart, 2006; Yoon, 2009]. Although high PDI countries have higher tolerance for unequal distribution of power in their society, high PDI also generates higher mistrust for powerful groups such as a company [Bellman *et al.*, 2004]. Thus, this finding implies that Indians would have less trust in e-commerce companies and should be less willing to disclose their personal information to web sites compared to the Americans because of the influence of power distance. Bellman *et al*. [2004] show similar findings for individualistic countries such as the U.S., where people are more comfortable in disclosing their personal information online. A cross-cultural study of consumers from the U.S. and Hong Kong (a higher collectivistic culture compared to the U.S.) found that Hong Kong consumers had higher levels of concerns for both online privacy and security [Greenberg, Wong-On-Wing and Lui, 2008].

Based on the above discussion and the differences in the individualism and power distance dimension indices between India and the U.S., it would be reasonable to predict that Indian consumers are less likely to be willing to share their personal information during online transactions because they are wary of entities such as a company and are less likely to trust people outside of the extended family and friends. We can thus formulate the proposition that the Indian consumers should be less willing to disclose personal information than the Americans.

H1: Consumers from India are less willing to disclose personal information (WDPI) online than the consumers from the U.S.

Since we have hypothesized that there are differences in WDPI between the two countries (see H1), we test if there are differences in the types of personal information disclosed that predict privacy protection behavior intentions and actual privacy protection actions for Indian and American consumers.

H2a: Willingness to disclose different types of personal information predicting intention to engage in privacy protection behavior will differ between India and the U.S.

H2b: Willingness to disclose different types of personal information predicting actual privacy protection actions will differ between India and the U.S.

In comparing the U.S. and Korea, Choi and Geistfeld [2004] show that higher collectivistic cultures such as Korea have lower risk perceptions compared to higher individualistic countries such as the U.S. Collectivistic cultures do not place as much value on personal privacy as individualistic cultures do because people in collectivistic cultures are comfortable with sharing their personal thoughts, beliefs, and trust *within* their family and community but not necessarily with people outside of their extended family [Choi and Geistfeld, 2004]. This diluted emphasis on personal privacy in collectivistic cultures manifests as reduced perceived risk as people rely on their family, friends, and society to bear the negative consequences of risk [Choi and Geistfeld, 2004], hence they may be taking less protective actions when engaging in risky behavior. Thus, more collectivistic cultures such as India may be associated with lower levels of perceived risks compared to individualistic cultures such as the U.S.

Higher collectivistic cultures that do not perceive personal privacy as strongly as individualistic cultures also have a higher acceptance for entities such as companies intruding upon an individual's privacy compared to more individualistic cultures [Bellman *et al*. 2004]. This acceptance would suggest that consumers from high collectivistic index cultures would be less concerned about their privacy and would also have lower levels of perceived online risks compared to consumers from individualistic societies.

People in cultures with higher long term orientation such as India have beliefs in future rewards that allow them to take risks during uncertainty or vulnerability, as opposed to people from low long term orientation cultures such as the U.S. [Yoon, 2009]. This longer term orientation may suggest that Indian consumers may not be as concerned in taking protective actions because risks of negative consequences such as loss of privacy are reduced by the characteristics of their long term orientation culture.

As discussed in Section 2.1, consumers with higher perceived risks and privacy concerns are likely to have higher intentions to engage in more privacy protective actions. Based on the above discussion we expect that the consumers from more collectivistic and higher long term orientation cultures such as India will have lower perceived risks and privacy concerns and therefore, less likely to engage in taking privacy protective actions compared to consumers from the more individualistic and high short-term orientation cultures such as the U.S. We can thus formulate the following set of hypotheses about relationship between consumers from differing cultures and their intentions to take privacy protective actions, and their likelihood of actually taking protective actions in the present.

H3: Consumers from India are likely to have lower intention to engage in privacy protection actions compared to the consumers from the U.S.

H4: Consumers from India are less likely to be practicing actual privacy protection actions compared to the consumers from the U.S.

H5: The relationship between intention for privacy protection actions and actual actions will be stronger for consumers from the U.S. compared to the consumers from the India.

3. Research Methodology

3.1. Survey Development

Participants completed a survey designed to obtain online consumers' willingness to disclose various types of personal information, their intentions and actual practices in protecting privacy as well as securing their personal information, offline and online. We adapted most of the measurement scales for research constructs from already validated constructs from earlier studies, notably, the work of Phelps *et al.* [2000]. The survey also included multiple items to measure privacy and security protection constructs - consumers' intention to protect their privacy, intentions to secure their information, actual practice to protect their privacy, and secure their information. We use the national-level analysis for measuring the culture differences consistent with the work of Hofstede [1984] as well as many other subsequent cross-cultural studies citing social identification theory [Gefen and Heart, 2006; Sia, Lim, Leung, Lee, Huang and Benbasat, 2009].

3.2. Data Collection and Demographics

Fifteen subjects in the U.S. and India served as pilot samples to establish content validity, clarity and precision of the survey. The survey was refined based on pilot data feedback. Survey was in English for both countries. In the U.S., survey was administered to students, faculty, staff and greater university communities in two cities. In India, we used a snowball technique to collect responses from people in universities, offices, and residential areas in five cities. For the snowball technique, initial participants were asked to recommend others who might be willing to participate in a survey about online experiences and transactions. Subsequently, the recommended individuals were approached to participate in the study. Respondents self-reported several demographics and the descriptive statistics are in Table 2.

Table 2: India vs. the U.S. - Descriptive Statistics of Respondents

	USA	India
Responses	267 (33%)	542 (67%)
Gender		
• Male	50%	70%
• Female	50%	30%
Age (in years)		
• 18-35	82%	79%
• >35	18%	21%
Education		
• Bachelors or less	88%	47%
• Graduate	12%	53%
Occupation		
• Employed	45%	47%
• Student	52%	51%
• Other	3%	2%
Over 3 years of average Internet use	92%	52%

4. Data Analysis and Results

4.1. Measures Validation

Willingness to disclose personal information (WDPI): Participants rated thirteen items (adapted from [Phelps *et al*, 2000]; [Sheehan and Hoy, 2000]) of personal information from 1 (not at all willing) to 5 (very willing). For the US respondents, Cronbach's alpha was .88; for the Indian respondents, the alpha was .87.

Measure development for intentions in ensuring and protecting privacy: Respondents rated six items (1 = highly unlikely to 5 = very likely) on their intentions that related to privacy and security of their personal information during online transactions (adapted from [Phelps *et al*, 2000]; [Sheehan and Hoy, 2000]). Cronbach's alpha for the entire scale was .66. To verify the structure of the scale, a factor analysis was conducted. Two factors

emerged in the initial solution with eigenvalues above 1. A follow up analysis was conducted with Varimax rotation to separate the items into two separate, orthogonal scales.

Three items (intention to read website's privacy policy, and intention to read website's security policy before making any online purchase, and intention to use software using virus protection, firewall, etc. to protect their personal information on the computer system) loaded on one factor with loadings of .77, .89, and .57 respectively. Even though one item loading was below recommended minimum value of .6 [Chin, Gopal, and Salisbury, 1997], we decided to attach it to this factor as item loading was greater than 0.5. In examining these three items, the underlying construct seems to be around passive online activities – reading policies and using virus protection software, without requiring strong intervention from the user. These three items comprised the subscale of *Intention for Passive Protection (IPP)* with Cronbach's alpha of .67 for the American sample and .68 for the Indian sample.

Three items (intention to provide misleading information during online registration, intention to opt out from the email list during online registration and intention to periodically delete cookie files from their computers) loaded onto another factor with factor loadings of .68, .81, and .65 respectively. In examining these three items, the underlying construct seems to be around active processes user needs to engage in to ensure their privacy and protect it. These items became the *Intention for Active Protection (IAP)* subscale with Cronbach's alpha of .58 for the American sample and .55 for the Indian sample.

Measure development for actual practices with online protections: Respondents rated six items (1 = strongly disagree to 5 = strongly agree) that paralleled intention in online protection items (adapted from [Phelps *et al*, 2000]; [Sheehan and Hoy, 2000]]. These items were worded towards the current online transactions practice such as buying, registering etc. and are self-reported by the respondents. We also analyzed the underlying factor structure to verify the structure of the construct. Since similar items as the Intentions items were used in this scale, they also loaded onto two factors that paralleled the Active and Passive dimensions as in the Intentions scales. We then completed a factor analysis with Varimax rotation for the two factors. Three items, "I frequently read the company's online privacy policy," "I use software (e.g. virus protection, firewall, etc.) to protect my personal information on the computer system," and "I frequently read a company's online security policies before making an online purchase from them" (loadings of .72, .63, .88, respectively) corresponded to IPP subscale, and therefore formed the subscale of *Passive Protection Actions (PPA)* with Cronbach's alpha of .64 for the American sample and .64 for the Indian sample.

Three items, "I frequently provide false personal information," "I frequently opt out from the email or marketing lists," and "I frequently delete cookie files from my computers" corresponded to IAP subscale, and therefore became the *Active Protection Actions (APA)* subscale (loadings of .72, .63, and .88) with Cronbach's alpha of .71 for the American sample and .67 for the Indian sample.

The IPP and IAP scales assess individuals' intentions to engage in passive and active protection. Items begin with "I intend to" and conclude with behaviors such as "read the company's online privacy policy before making any online purchases from them," "opt out from the email list during registration," and "periodically delete cookie files from my computers. The PPA and APA scales assess individuals' actual behavior during online transactions. The items are the same but without the preceding "I intend to." Examples for the PPA and APA are "I frequently read the company's online privacy policy" and "I frequently opt out from email/marketing lists." Conceptually, the former measures intentions and the latter actions. The intention scales (IPP and IAP) and the action scales (PPA and APA) are closely associated, indicating a conceptual link (See Table 3).

Table 3: Correlations of intentions for protective actions (IPP & IAP) and actual protective actions (PPA & APA)

	IPP	IAP	PPA	APA
1. IPP		.31***	.56***	.23***
2. IAP			.20***	.68***
3. PPA				.42***
4. APA				

* p < .05, ** p < .01, *** p < .001.

4.2. Differences between the U.S. and Indian consumers

Willingness to disclose personal information (WDPI) online: American participants were most willing to disclose their media habits, name, and email address. Indian consumers reported most willingness to disclose media habits, email address, demographic and lifestyle data. In order to test differences between the U.S. and Indian samples on willingness to disclose certain types of information, *t*-tests were conducted on the thirteen items.

Americans reported greater willingness to disclose their less sensitive information like their names (M = 3.40, SD = 1.29) than did Indians (M = 3.15, SD = 1.57), *t* (617) = -2.49. Indians also were more willing to disclose more sensitive personal information such as their date of birth, work address, work phone number, home phone number, medical history and financial information than Americans (see Table 4). Thus, H1 is supported for less sensitive information but not for more sensitive information.

Predicting Intentions for Passive and Active Protection, and Passive and Active Protection Actions: In order to assess (H2a and H2b) if willingness to disclose certain types of personal information predicts intention to engage in passive and active protection, and actual passive and active protective actions taken, a series of stepwise multiple regressions were conducted separately for the U.S. and Indian samples.

Analyses for the U.S. sample indicated that the linear combination of greater willingness to disclose credit card information and less willingness to disclose home address predicted intention for passive protection (IAP), the linear combination of greater willingness to disclose email and less willingness to disclose medical information predicted active protection actions (APA) taken. Intention for active protection (IAP) was best predicted by willingness to disclose email and less willingness to disclose financial information. See Table 5 for details.

For the Indian sample, intention for active protection (IAP) is predicted by willingness to disclose name, email address, media habits and less willingness to disclose credit information; and intention for passive protection (IPP) is predicted by willingness to disclose name and email and less willingness to disclose credit information and home address. Passive protection actions (PPA) are best predicted by willingness to disclose name and home address. Active protection actions (APA) are best predicted by willingness to disclose name and email and less willingness to disclose credit information. See Table 6 for details.

Table 4: Comparison of WDPI between the U.S. and India Consumer Samples.

Type of personal information	US Sample *M (SD)*[†]	India Sample *M (SD)*	t (df)
Media habits	3.58 (1.32)	3.51 (1.42)	-.62 (561.13)
Name	**3.40** (1.29)	3.15 (1.57)	-2.49 (617.36)**
Email address	3.29 (1.27)	3.42 (1.44)	1.29 (588.55)
Lifestyle data (own or rent home, number of pets, etc.)	3.13 (1.32)	3.20 (1.38)	-.74 (802)
Demographic Data (e.g., age, weight, ethnicity, etc.)	3.03 (1.32)	3.20 (1.38)	1.64 (804)
Date of birth	2.53 (1.37)	**2.97** (1.44)	4.12 (801)***
Home address	2.53 (1.34)	2.56 (1.41)	.29 (804)
Work address	2.45 (1.31)	**2.80** (1.37)	3.50 (802)***
Work phone number	2.37 (1.31)	**2.65** (1.43)	2.77 (560.52)**
Home phone number	2.11 (1.26)	**2.33** (1.34)	2.24 (552.29)*
Credit card details	2.02 (1.17)	1.89 (1.15)	-1.45 (803)
Medical history	1.84 (1.12)	**2.66** (1.35)	9.13 (619.97)***
Financial information (income, credit history, etc.)	1.66 (.96)	**2.10** (1.29)	5.42 (677.97) ***

Note. [†]1 = not at all willing to 5 = very willing. * p < .05, ** p < .01, *** p < .001.

Table 5: Combined regression for Intentions for Active Protection (IAP) and Intentions for Passive Protection (IPP) and Active Protection Actions (IPA) and Passive Protection Actions (PPA) for the U.S. sample.

U.S.		B	SE	Beta
Intention for Passive Protection (IPP)	Credit	.24	.06	.29***
	Home address	-.14	.05	-.20**
Intention for Active Protection (IAP)	Email	.12	.05	.15*
	Financial	-.14	.07	-.14*
Passive Protection Actions (PPA)	Credit	.24	.06	.30***
	Home address	-.16	.05	-.24**
Active Protection Actions (APA)	Medical	-.17	.06	-.20**
	Email	.11	.05	.14*

* p < .05, ** p < .01, *** p < .001.

Table 6: Combined regression for Intentions for Active Protection (IAP) and Intention for Passive Protection (IPP) and Active Protection Action (IPA) and Passive Protection Actions (PPA) for the India sample

India		B	SE	β
Intention for Passive Protection (IPP)	Credit	-.07	.03	-.09*
	Email	.08	.03	.14**
	Home address	-.15	.04	-.24***
	Name	.11	.03	.21**
Intention for Active Protection (IAP)	Email	.18	.04	.24***
	Name	.15	.03	.22***
	Credit	-.14	.04	-.15***
	Media	.08	.03	.10*
Passive Protection Actions (PPA)	Name	.16	.03	.28***
	Home address	-.12	.04	-.19**
Active Protection Actions (APA)	Email	.17	.04	.23***
	Name	.13	.03	.19***
	Credit	-.11	.04	-.11**

* p < .05, ** p < .01, *** p < .001.

Thus, analyses in tables 5 and 6 show that there are differences among Indian and U.S. consumers on type of personal information predicting intentions to engage in privacy protection behavior and actual protective actions taken, supporting H2a and H2b.

Difference in Intention for Passive and Active Protection (IPP & IAP), and Passive and Active Protection Actions (PPA & APA): In order to assess the differences in the intentions for protection and actual actions being taken during online interactions between the U.S. and Indian sample, an analysis of variance was conducted to test H3 and H4. Analyses (see Table 7) revealed that Americans report engaging in more intentions for passive protection, IPP (M = 3.51, SD = 95) and more passive protection actions, PPA (M = 3.45, SD = 93), than do the Indian participants (M = 3.06, SD = .88 and M = 3.02, SD = .89, respectively), $F\ (1, 792) = 44.27$, $p < .001$ and $F\ (1, 794) = 39.68$, $p < .001$, respectively. Hypotheses H3 and H4 are both supported for intention and action for passive protection but not for intention and action for active protection.

Table 7: ANOVA Results, Means, and Standard Deviations of IPP, IAP, PPA, and APA by country

	U.S. *M (SD)*[†]	India *M (SD)*	
Intention for Passive Protection (IPP)	3.51 (.95)	3.06 (.88)	F (1, 792) = 44.27 ***
Intention for Active Protection (IAP)	3.56(1.00)	3.59 (1.06)	F (1, 792) = .21
Passive Protection Actions (PPA)	3.45 (.93)	3.02 (.89)	F(1, 794) = 39.68***
Active Protection Actions (APA)	3.43 (.97)	3.33 (1.07)	F (1, 794) = 1.61

[†] 1 = Not at all willing to 5 = very willing. * p < 05, ** p < .01, *** p < .001.

Next, we analyzed the intercorrelations of two subscales of protection intentions, IAP and IPP, and two subscales of protection actions, PPA and APA, in the U.S. and India (see Table 8).

Table 8: Inter-correlations of Intentions for Passive Protection (IPP) and Intention for Active Protection (IAP) and Passive Protection Actions (PPA) and Active Protection Actions (APA) in the U.S. and India.

	Intention for Passive Protection (IPP)	Intention for Active Protection (IAP)	Passive Protection Actions (PPA)	Active Protection Actions (APA)
	U.S. (India)	U.S. (India)	U.S. (India)	U.S. (India)
Intention for Passive Protection (IPP)	---	.33*** (.32***)	.79*** (.41***)	.32*** (.18***)
Intention for Active Protection (IAP)		--	.22*** (.20***)	.82*** (.62***)
Passive Protection Actions (PPA)			--	.31*** (.47***)
Active Protection Actions (APA)				--

* p < .05, ** p < .01, *** p < .001

For the U.S. sample, the Intention for Passive Protection (IPP) and the Passive Protection Actions (PPA) are strongly associated (*r = 0.79, p< 0.001*). The relationship between Intention for Active Protection (IAP) and Active Protection Actions (APA) is the same (*r = 0.82, p<0.001*). In the Indian sample, the relationship between intentions and actions is still statistically significant (*r = 0.41, p< 0.001; r = 0.62, p< 0.001)* but is not as strong as in the U.S. sample. It is evident from Table 8 that hypothesis H5 is supported. That is, the relationship between intentions and actions for the U.S. consumers is stronger (*r = 0.79 and r = 0.82*) than for the Indian consumers (r = *0.41 and r = 0.62*).

Thus, we found partial support for H1 (the U.S. respondents were more willing to provided less sensitive information where as Indian respondents were willing to disclose more sensitive information) and for H3 and H4 (consumers from India have lower intentions and take less actual passive protection actions compared to the U.S. consumers) but not for active protection intentions and actions. H2a and H2b are statistically supported (there were differences between WDPI and privacy protection intentions and actions between Indian and U.S. consumers) and H5 (relationship between intentions and actions for privacy protection are stronger for the U.S. consumers than Indian consumers).

5. Discussion

In considering the role of culture on the consumers' WDPI in India and the U.S., we find that the Indian consumers are more willing to disclose potentially sensitive personal information such as date of birth, work address and phone number, home phone number, medical history and financial history than the U.S. consumers. This greater willingness suggests that there are significant differences in what personal information Indian and the U.S. consumers perceive as sensitive or risky that would make them vulnerable to adverse consequences as a result of the disclosure. Thus, culture seems to be a significant factor in WDPI. In India, because of its collectivistic culture, consumers may be more willing to extend and preserve their relationship with an organization because it is seen as part of an extended community represented through a website. Consequently, their desire to maintain the relationship is realized through sharing of personal information. In the U.S., however, consumers are more individualistic and may not be as invested in developing a relationship with an e-business unless it was for self-interest purposes. In collectivistic India, people routinely share their date of birth, income, marital status, and political affiliation etc. with people they may know only slightly. It is common, for example, for Indian job applicants to post their resumes online with all their personal details, different from the cultural practice in the U.S. Culturally, therefore, Indians may not conceive of a potential for malicious behavior in disclosing personal information online to a company. These cultural differences in what is perceived to be sensitive personal information are reflected in the results we obtained. This finding lends credence to the phenomenon of "group diffusion effect" that posits that collectivistic cultures, such as India, tend to exhibit lower privacy concerns (more willingness to share sensitive personal information). A collectivist society can provide a greater cushion in the form of in-group members that can help mitigate possible negative consequences of lower privacy concerns [Choi and Geistfeld, 2004].

In considering the role of culture in intention and actions being taken for *active protection*, i.e., providing false information, frequently opting-out from marketing lists, and frequently deleting cookies from their computer across two countries, we find no significant differences. Consumers from both countries exhibit relatively high intentions and report more actions (IAP & APA) being taken for active protection while online. However, there were significant differences in intention and actions for passive protection (IPP & PPA), i.e., frequently reading privacy and security policies, and using software to protect personal information, across both nations, with the U.S. consumers intending to and engaging in higher passive protection compared to Indians. These significant

differences between the U.S. and Indian consumers regarding passive protections, IPP and PPA, suggests that since Indian culture places higher trust in institutions, Indian consumers may be more trusting of an online company than American consumers, and thus may not feel the need to read privacy and security policies. It could also be that because Americans have higher levels of the Internet experience, American online consumers may be more cognizant of actions to take to ensure and protect their privacy, whereas Indian consumers may not yet be as sensitive to the role of a company's privacy and security policies.

We also find that the U.S. consumers with higher intentions to protect their online privacy engaged in more protective practices than the Indian consumers. This suggests that of those Indian consumers who expressed higher intent to protect their privacy, most were not actually taking these protective actions at present. This disparity may be a reflection of the long-term orientation and uncertainty avoidance differences in these two cultures where Indians with long-term orientation and lower uncertainty avoidance may see themselves at some future point engaging in protecting their online privacy; they do not, however, consider it as an immediate risk or need.

In considering our results on the types of information disclosed predicting a consumer's protective behavior, we find that the U.S. consumers understand that divulging sensitive information such as credit card account numbers requires broader protections, those we called passive protective actions, like reading policies and using virus protection software. Those in the U.S. who are divulging their email address are more aware of the need to engage in active protection such as providing false information, frequently opting-out from marketing lists, and frequently deleting cookies from their computer. For the Indian consumers, those who are willing to disclose email address and their name intend to engage in passive protective actions. For Indian sample, sharing email and name may trigger higher concern for ensuring and protecting their privacy.

Willingness of Indian consumers to disclose sensitive personal information may suggest that some consumers in India are not yet concerned about divulging personal information, leaving them open to exploitation by unscrupulous online firms. This willingness to disclose may be due the fact that e-commerce is still a relatively new marketing channel and only a very small population is currently engaged in it. Another explanation is that Indian consumers may not have experienced the adverse consequences yet from divulging too much personal information and therefore may be more willing to disclose personal information. In addition, the credit card is a new financial tool in India and most consumers still use cash for most of their purchases [Mishra, 2007]. Therefore, Indian consumers may not be as aware or concerned about credit ratings, and thus, about the identity theft. As credit card for EC use continues to increase, Indian consumers may be less readily willing to share personal information online.

In this study, our findings are limited to consumers representing two distinct cultures: the U.S. and India. Also, we used the culture measures at national level as published by Hofstede [2001] and not at the individual level on the culture dimensions. While prior studies on cultural comparisons [Muthitacharoen and Palvia, 2002] have done the same, using the culture index of a country might possibly ignore individual differences in a particular culture [Myers and Tan, 2002].

6. Implications and Future Research

In general, consumers are becoming more self-reliant about protecting their personal information online. In comparing the two countries with distinct cultural and ICT profile, Indian consumers are more willing to share sensitive information online than the U.S. counterparts. Also, consumers from India were less likely to be engaging in protective behaviors compared to consumers in the U.S.

When companies understand when and under what circumstances consumers will disclose certain types of information, they can then design websites that foster consumer trust. This helps companies elicit consumers' personal information and provide them with enhanced services. Companies that target the U.S. consumers may need to provide stronger privacy and security policies and measures to enhance consumer trust. That may encourage the U.S. consumers to be more willing to disclose their personal information online. Companies that target Indian consumers should understand that in India, with its cultural orientation towards collectivism, investments in fostering relationships with their consumers may gain consumers' brand loyalty because the website is viewed as an extension of the individuals' trusted community. For global companies, understanding the role of culture in online information disclosure behavior implies that they cannot use the same policies and practices for all customers worldwide since consumers from different cultures have different notions of sensitive information and its disclosure. Using this localization approach that incorporates cultural aspects of a target market, companies can better segment their market and develop appropriate marketing strategies. Companies can be more innovative in seeking more specific information from consumers.

Future research that considers cultural dimensions at an individual level may provide greater understanding of specific cultural dimensions that may be dominant in online consumer behavior. Another research avenue would be to give consideration to subcultures rather than assuming that cultures are homogeneous.

REFERENCES

Bellman, S., E.J. Johnson, S.J. Kobrin, and G.L. Lohse, "International Differences in Information Privacy Concerns: A Global Survey of Consumers," *The Information Society*, Vol.20, 313–324, 2004.

Brown, M. and R. Muchira, "Investigating the Relationship between Internet Privacy Concerns and Online Purchase Behavior," *Journal of Electronic Commerce Research*, Vol.5, No.1:62-70, 2004

Castañeda, J. A. and F. J. Montoro, "The effect of Internet general privacy concern on customer behavior," *Electronic Commerce Research*, Vol. 7, No. 2:117-141, 2007.

Chin, W.W., A. Gopal, and W.D. Salisbury, "Advancing the theory of adaptive structuration: The development of a scale to measure faithfulness of appropriation," *Information Systems Research*. Vol. 8, No. 4:342-367, 1997.

Choi, J and L.V. Geistfeld, "A cross-cultural investigation of consumer e-shopping adoption," *Journal of Economic Psychology*, Vol.25:821–838, 2004.

Earp, J. B., and D. Baumer, "Innovative web use to learn about user behavior and online privacy," *Communications of the ACM*, Vol.46, No.4:81–83, April 2003.

Fusilier, M. and S. Durlabhji, "An exploration of student internet use in India: the technology acceptance model and the theory of planned behavior," *Campus - Wide Information Systems*, Vol.22, No.4:233-246, 2005.

Gauzente, C. "Web merchants' privacy and security statements: how reassuring are they for consumers? A two-sided approach," *Journal of Electronic Commerce Research*, Vol.5, No.3:181-198, 2004.

Gefen, D. and T. Heart, "On the Need to Include National Culture as a Central Issue in E-Commerce Trust Beliefs," *Journal of Global Information Management*, Vol.14, No.4:1-30, 2006.

Greenberg, R., B. Wong-On-Wing and G. Lui, "Culture and Consumer Trust in Online Businesses," *Journal of Global Information Management*, Vol.16, No.3:26-44, 2008.

Hann, I., K. Hui, S.T. Lee and I.P.L. Png, "Overcoming Online Information Privacy Concerns: An Information-Processing Theory Approach," *Journal of Management Information Systems*, Vol. 24, No. 2:13–42, 2007.

Hofstede, G., Culture's Consequences, Beverly Hills, CA: Sage Publications, 1984.

Hofstede, G., Culture's Consequences: International Differences in Work-related Values, Sage, London, 2001.

Internet World Statistics: Usage and Population Statistics (2009), Retrieved on Jan 15, 2009 from http://www.internetworldstats.com/stats.htm.

Kivijärvi, M., T. Laukkanen and P. Cruz, "Consumer Trust in Electronic Service Consumption: A Cross-Cultural Comparison Between Finland and Portugal," *Journal of Euromarketing*, Vol.16, No.3:51-65, 2007.

Kumaraguru, P., L.F. Cranor, and E. Newton, "Privacy Perceptions in India and the United States: An Interview Study," In *The 33rd Research Conference on Communication, Information and Internet Policy (TPRC)*, Sep 23 -25, 2005.

Lanier, C.D. Jr. and A. Saini, "Understanding Consumer Privacy: A Review and Future Directions," *Academy of Marketing Science Review*, Vol. 12, No. 2:1-49, 2008.

Lauer, T.W. and X. Deng, "Building online trust through privacy practices," *International Journal of Information Security*, Vol. 6, No. 5:323-331, 2007.

Lwin, M., J. Wirtz, and J.D. Williams, "Consumer Online Privacy Concerns and Responses: A Power-Responsibility Equilibrium Perspective," *Journal of the Academy of Marketing Science*, Vol 35, No 4:572-585, 2007.

Meinert, D.B., D.K. Peterson, J.R. Criswell and M.D. Crossland, "Privacy Policy Statements and Consumer Willingness to Provide Personal Information," *Journal of Electronic Commerce in Organizations*, Vol.4, No.1:1-17, 2006.

Mishra, G., "Credit card use in India lowest in world," The Economic Times, http://economictimes.indiatimes.com/Personal_Finance/Credit_Cards/Credit_card_use_in_India_lowest_in_world/rssarticleshow/2088097.cms, 2007.

Muthitacharoen, A. and P. Palvia, "B2C Internet Commerce: A Tale of Two Nations," *Journal of Electronic Commerce Research*, Vol. 3, No. 4:201-212, 2002.

Myers, M.D and F.B. Tan, "Beyond models of national culture in information systems research," *Journal of Global Information Management*, Vol.10, No.4:24-32, 2002.

Nam, C., C. Song, E. Lee and C.I. Park, "Consumers' Privacy Concerns and Willingness to Provide Marketing-Related Personal Information Online," *Advances in Consumer Research*, Vol 33, 212-217, 2006.

Painea, C., U. Reipsb, S. Stiegerc, A. Joinsona, and T. Buchanan, "Internet users' perceptions of 'privacy concerns' and 'privacy actions'." *International Journal Human-Computer Studies*, Vol.65, No.6:526–536, 2007.

Pavlou, P.A. and L. Chai, "What Drives Electronic Commerce across Cultures? Across-Cultural Empirical Investigation of the Theory of Planned Behavior," *Journal of Electronic Commerce Research*, Vol.3, No.4:240-253, 2002.

Phelps J., G. Nowak, and E. Farrell, "Privacy Concerns and Consumer Willingness to Provide Information," *Journal of Public Policy and Marketing*, Vol.19, No.1: 27-41, 2000.

Rudraswamy, V. and D.A. Vance, "Transborder data flows: adoption and diffusion of protective legislation in the global electronic commerce environment," *Logistics Information Systems*, Vol.14, No.1&2:127-136, 2001.

Schulz, M. "Credit cards around the world: India," http://www.creditcards.com/credit-card-news/credit-cards-around-the-world-india-1276.php, 2008.

Sheehan, K.M. and M.G. Hoy, "Dimensions of Privacy Concern Among Online Consumers," *Journal of Public Policy and Marketing*, Vol.19, No.1: 62-93, 2000.

Sheng, H., F.F. Nah and K. Siau, "An Experimental Study on Ubiquitous commerce Adoption: Impact of Personalization and Privacy Concerns," *Journal of the Association for Information Systems*, Vol. 9, No 6:344-376, 2008.

Sia, C.L., K.H. Lim, K. Leung, M.K.O. Lee, W.W. Huang and I. Benbasat, "Web Strategies to Promote Internet Shopping: Is Cultural-Customization Needed?," *MIS Quarterly*, Vol.33, No.3:491-512, 2009.

Singh, N. and D.W. Baack, "Studying cultural values on the web: a cross-cultural study of U.S. and Mexican websites," *Journal of Computer Mediated Communication*, Vol. 9, No. 4, 2004.

Singh, N., O. Furrer and M. Ostinelli, "To Localize or to Standardize on the Web: Empirical Evidence from Italy, India, Netherlands, Spain, and Switzerland," *Multinational Business Review*, Vol.12, No.1:69-87, 2004.

Singh, N., G. Fassott, H. Zhao, and P.D. Boughton, "A Cross-cultural analysis of German, Chinese and Indian consumers' perception of web site adaptation," *Journal of Consumer Behaviour*, Vol.5, No.1: 56-68, 2006.

Son, J. and S.S. Kim, "Information Privacy-Protective Responses," *MIS Quarterly*, Vol.32, No.3: 503-529, 2008.

The Global Information Technology Report, http://www.weforum.org/en/initiatives/gcp/Global%20Information%20Technology%20Report/index.htm, 2009.

Van Slyke, C., F. Belanger and V. Sridhar, "A Comparison of American and Indian Consumers Perceptions of Electronic Commerce," *Information Resources Management Journal*, Vol.18, No.2:24-40, 2005.

Woolsey, B. and M. Schulz, "Credit card statistics, industry facts, debt statistics," http://www.creditcards.com/credit-card-news/credit-card-industry-facts-personal-debt-statistics-1276.php#topofpage, 2009.

Yoon, C, "The effects of national culture values on consumer acceptance of e-commerce: Online shoppers in China," *Information & Management*, Vol.46, No.5:294-301, 2009.

Zhang, X. "What Do Consumers Really Know," *Communications of the Association for Computing Machinery (CACM)*, Vol.48, No.8: 44-48, 2005.