

1-1-2009

Willingness to Disclose Personal Information Online and its Effect on Ensuring and Protecting Privacy: A Two Country Study

Babita Gupta

California State University - Monterey Bay, babita_gupta@csumb.edu

Lakshmi S. Iyer

University of North Carolina at Greensboro, Lsiyer@uncg.edu

Robert S. Weisskirch

California State University - Monterey Bay, rob_weisskirch@csumb.edu

Follow this and additional works at: <http://aisel.aisnet.org/amcis2009>

Recommended Citation

Gupta, Babita; Iyer, Lakshmi S.; and Weisskirch, Robert S., "Willingness to Disclose Personal Information Online and its Effect on Ensuring and Protecting Privacy: A Two Country Study" (2009). *AMCIS 2009 Proceedings*. Paper 172.

<http://aisel.aisnet.org/amcis2009/172>

This material is brought to you by the Americas Conference on Information Systems (AMCIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in AMCIS 2009 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

Willingness to Disclose Personal Information Online and its Effect on Ensuring and Protecting Privacy: A Two-Country Study

Babita Gupta

California State University Monterey Bay
babita_gupta@csumb.edu

Lakshmi S. Iyer

University of North Carolina Greensboro
lsiyer@uncg.edu

Robert S. Weisskirch

California State University Monterey Bay
rob_weisskirch@csumb.edu

ABSTRACT

Organizations rely on information disclosed by consumers during online interactions to render personalized services which can enhance the online experience. There are implications for businesses when consumers are willing to disclose information and subsequently, think about and act in ways to ensure and protect their privacy. In the global context, these concerns are magnified as companies rely on global networks to do business in other countries, and there are no international laws that adequately protect security of information. In this study, we conduct an empirical study of 809 consumers in U.S. and India to understand their information disclosing behavior online, their intentions to take and execution of protective actions during online interactions. Results suggest that there are differences between U.S. and India with regards to consumers' willingness to disclose personal information, and their intentions and actions for privacy and security protection. Differences in how willing consumers are to disclose information and in how concerned they are with protecting themselves has implications for companies in considering local cultures when conducting international e-commerce.

Keywords

Online privacy, security, information sharing, e-commerce, country differences, U.S., India.

INTRODUCTION

Consumers from all strata of society are increasingly participating in online interactions as a means for communicating and conducting transactions. During most interactions, they are asked to disclose different types of personal information so that organizations can provide better and personalized services. Organizations also rely on information disclosed by consumers during online transactions to develop strategies to enhance their online experience. Despite different strategies organizations use to enhance online interaction experience and thereby increase online sales, the percent of online retail sales compared to total retail sales is still a small percent, 3.3% by end of 4th quarter in 2008 in the United States (US Census, 2009), a nation which ranks high in internet penetration rate (Internet World Statistics 2009). Thus, the potential and opportunities for companies to leverage the online channel to increase revenues is high. However, research indicates that issues such as privacy and security of networks and encryption policies influence adoption and success of electronic commerce practices (Painea, Reipsb, Stiegerc, Joinsona & Buchanan, 2007).

Among consumers purchasing online, the overwhelming concern has been online privacy and security (Horrigan, 2008; Ahuja, Gupta and Raman, 2004) and how personal data would be used by the site collecting the information (Han and Maclaurin, 2002). Painea et al (2007) showed that online users were concerned about a wide range of privacy issues but their results did not provide final definitions for privacy actions. Federal guidelines for collection of personal information online from consumers rely on e-commerce sites to self-regulate themselves in protecting consumers' information privacy (Ackerman, 2009). While the U.S. has some data protection laws, such Federal level regulations and laws are still lacking in developing nations (Kumaraguru, Cranor and Newton, 2005). Cultural differences among nations are related to the degree of privacy sensitivity and privacy concerns for data protection of their citizens or corporations and are known to strongly correlate to regulatory approaches of a nation (Rudraswamy and Vance, 2001). Although there are studies in the U.S. that have looked at the willingness of consumers to disclose personal information online (Son and Kim, 2008; Earp and Baumer, 2003), there has been little research that compares consumer attitudes towards sharing information during online interactions across countries with varying privacy and security policies and regulations (Meinert, Peterson, Criswell and Crossland, 2006). This lack of research is important for two reasons. One, global companies need to better understand the differences in consumer intention and practices towards privacy and security protection based on their willingness to disclose information

for e-commerce growth. Second, since U.S. companies have outsourcing contracts with Indian companies, understanding the protective intentions and actions of Indian users regarding personal information is critical to sustaining business profitability. Based on a recent study, Kumaraguru et al. (2005) showed that Indians and Americans have differing levels of concern about privacy, and that the U.S. consumers are more aware of privacy issues. However, their study did not explore the specific differences between these two diverse groups of consumers with regards to personal information disclosure and consumers' protective intentions and actions. In our study, we compare consumers in the U.S. and India and their willingness to disclose personal information and consequent intentions and practices to protect their information. Beliefs and attitudes are subjective elements of culture dimensions. Based on studies by Hofstede and Hofstede (2004) and House, Hanges, Javidan, Dorfman & Gupta (2004), U.S. and India fall under two distinct cultural groups based on varied cultural dimensions. For example, the power distance index for India is 77 while that of US is 40 and on the individualism scale, India's score is 42 while that of U.S. is 91¹.

This study has implications for global e-commerce companies and may provide ways for these companies to address consumers' privacy and security concerns so that consumer are more willing to disclose personal information that will help companies offer enhanced services to their customers, increase their pool of potential consumers, and increase sales.

LITERATURE REVIEW

Information Privacy and Security

Privacy of an individual, as advanced by Warren and Brandeis (1890) in their essay, is the right of an individual to protect personal details from any publication, whether obtained lawfully or unlawfully (What is Privacy, 2004). In the context of information privacy, it also denotes the right to control the conditions under which information about an individual is collected, used and disseminated (Malhotra, Kim and Agarwal, 2004; Westin, 1967). Federal government guidelines for fair information practices refer to five core principles of privacy protection: *notice/awareness; choice/consent; access/participation; integrity/security; and enforcement/redress* (Fair Information Practice, 2009). Information security, a subset of FTC privacy protection guidelines, is the process of protecting data from misuse by people and/or systems inside or outside of an organization (Berinato and Scalet, 2006). Privacy refers to the right of a person to control his or her own personal information (Kelly, 2000) whereas security refers to the ability of the owner of the information to keep it secure by protecting it from unauthorized access. Thus, "information is secure if the owner of information can control that information. Information is private if the subject of information can control that information." (Head and Yuan, 2001, pp 150).

Phelps, Nowak and Ferrell (2000) describe the four dimensions of privacy violations as: *intrusion, disclosure, false light and appropriation*, and the two types of control that most consumers want on their online information – how the collected information will be disseminated and how much marketing solicitations will result from this information.

As e-commerce proliferates, online privacy concerns arise regarding personal information collected about a consumer for a specific purpose like registering to get an email account, win free merchandise, providing a home or work address, credit card information etc. to complete an online purchase process, or providing detailed demographic and personal financial data when applying for an online loan or credit card. Combination of factors like advances in technologies, increasing value of personal information about consumers to marketers due to competitive pressures, evolution of marketing strategies like niche marketing, one-to-one marketing and other customization approaches are resulting in a perceptible erosion of consumer privacy (Rust, Kannan and Peng, 2002). 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; Milne, Rohm & Bahl, 2004).

Sheehan and Hoy (1999), in their study, reported that, as consumer's privacy concerns increase, online behavior changes. Consumers with high privacy concerns expect web merchants to indicate clearly how information security and control would be guaranteed (Gauzente, 2004). Increased privacy concerns lead to greater likelihood of consumers providing incomplete or false information to web sites, being more pro-active in opting out and less likely to register with web sites requesting information. However, the Sheehan and Hoy study neither considers privacy and security issues together nor provides granularity regarding the relationship between personal information disclosed and the impact on consumer's intention and actions regarding protection.

There have been some studies that consider national culture and its influence on Internet use and electronic commerce. Dinev, Bellotto, Hart, Russo, Serra and Colautti (2006) found that consumers in Italy exhibit lower Internet privacy concerns

¹ http://www.geert-hofstede.com/hofstede_dimensions.php, Accessed on April 16, 2009.

than consumers in the U.S., lower perceived need for government surveillance, and higher concerns about government intrusion. They also established that online privacy concerns and Internet users' attitudes toward government surveillance are significant predictors of e-commerce use for both countries. U.S. consumers find that government efforts to make the Internet safer influence their e-commerce use and they are more inclined to make online transactions because they would feel more secure. Website preferences of consumers in Germany, China and India and determined that consumers prefer culturally adapted local web sites, and that culture influences consumer's beliefs, attitudes and intention to buy online (Singh, Fassott, Zhao and Boughton, 2006). Fusilier and Durlabhji (2005) found that in a less individualistic culture such as India, social factors may be an important influence on behavior.

Bellman, Johnson, Kobrin, and Lohse (2004) found differences in how Internet privacy concerns are related to cultural values of nations and to differences in Internet experience. In addition, in one study, U.S. and Taiwanese consumer perceptions concerning online privacy and how it relates to the level of trust with a company's web site. The study found that trust is an important intermediary variable that influences behavioral intentions for online transactions (Liu, Marchewka and Ku, 2004).

Park and Jun (2003) found significant differences in Internet usage and the perceived risks of Internet shopping between Korean and American consumers. They also found that cultural difference has an effect on Internet usage and perceived risks on online buying behavior.

We consider two countries for our analysis, the U.S. and India. We chose these countries because they represent largely different cultures, are geographically distant, and are on different levels in terms Information and Communication Technology (ICT) infrastructure and e-readiness. Based on ICT use, economies of the world, each country is assigned an e-readiness level, Tier 1, Tier 2 and Tier 3, which indicates that country's level of free trade, industry self-regulation, ease of exports, and compliance with international standards and trade agreements. A country with higher level of e-readiness exhibits fewer barriers to electronic commerce growth. U.S. is ranked 2nd among considered an established leaders, Tier 1, while India is ranked 13th among late entrants, Tier 3 (Cortada, Gupta and Le Noir, 2007).

As of 2008, the U.S. had 72.4% of its population using the Internet while in India, only 5.2% of the population was online (Internet World Statistics, 2009). However, the growth rate of Internet users in India is more than a thousand percent over the last eight years which provides growth opportunities for global companies, particularly in e-commerce. Thus understanding the perceptions, intention and actions of this growing customer base merits study. We next present our research questions and methodology for this study.

RESEARCH QUESTIONS AND METHODOLOGY

This study aims to examine the relationship between consumers' willingness to disclose personal information online and how it influences their intention and actual practice in protecting their information from unauthorized use. We conducted an empirical study to explore the following research questions:

- What kind of personal information are consumers willing to disclose online, and what are they sensitive about sharing? Are there any differences among consumers in India and the U.S.?
- Does willingness to disclose certain type of personal information relate to consumers' intention to limit their privacy exposure and secure information? Are there country differences?
- Does willingness to disclose certain types of personal information relate to actual steps a consumer takes to limit privacy exposure and secure personal information? Are there country differences?
- What are the consumer's practices towards securing of their personal transactions online?
- How does a consumer's willingness to disclose certain types of personal information predict their protective intentions and practices?

Data collection and Analysis

A survey was designed to collect data on 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. Most of the measurement scales for research constructs were adapted from already validated constructs from earlier studies, notably, works of Phelps, Nowak and Ferrell (2000). Survey also included multiple items to measure privacy and security protection constructs - consumer's intention to protect their privacy, intentions to secure their information, actual practice to protect their privacy, and secure their information. These items used five-point Likert scale ratings of agreement from strongly disagree to strongly agree.

Data Collection

Survey was pilot tested with 15 subjects in the U.S. and India to establish content validity, clarity and precision. Based on pilot test feedback, the survey was refined. We collected a total of 809 valid responses over several months using paper survey (91%) from two cities in the U.S. and five cities in India, and online survey link (9%). Of these, 33% of responses (267) are from the U.S. and rest are collected from India (542). Respondents self-reported gender, age, highest level of education, occupational status, marital status, household income, and citizenship. Of these respondents, 62% are male, 36 % are females with 2% declining to state their gender. Majority of respondents are between 18-55 years old with 55% in 18-25 age groups, and 36% in 26-55 age groups. Average Internet use in the U.S. was higher than in India. There were significant differences between the U.S. and India on expected average time online per week. The U.S. sample reported more than 10 hours per week of Internet use while Indian sample reported equal to or less than five hours per week of Internet use. There was also a significant difference in two countries in the total amount of money spent in online purchases in previous six months because most Indians did not purchase anything online (65%) compared to 61% of the U.S. consumers spending more than \$50, $\chi^2(5) = 1.42, p < .001$.

Analysis and Results

Willingness to disclose personal information (WDPI) online. Participants rated thirteen items of personal information from 1 (not at all willing) to 5 (very willing) (see Table 1). As a scale, Cronbach's alpha was .87 for this sample. 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 US and Indian samples on willingness to disclose certain types of information, t-test were conducted on the thirteen items. Americans reported greater willingness to disclose their names ($M = 3.40, SD = 1.29$) than did Indians ($M = 3.15, SD = 1.57$), $t(617) = -2.49$. A single factor did not emerge from the unrotated factor solution consistently in each factor analysis, which does not indicate common method variance (Malhotra, Kim & Patil, 2006). Indians also were more willing to disclose their date of birth, work address, work phone number, home phone number, medical history and financial information than Americans (see Table 1).

Type of personal information	US Sample	India Sample	t (df)
	M (SD)†	M (SD)	
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 1: Willingness to disclose personal information

Measure development for intentions in ensuring and protecting privacy. Respondents rated six items from 1 = highly unlikely to 5 = very likely on their intentions in online transactions that related to privacy and security of their personal information. Cronbach's alpha for this 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 loaded on one factor (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) 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 great than 0.5. In examining these three items, underlying construct seems to be around passive activities – reading policies and using virus protection software, without requiring strong intervention from the user. These items comprised the subscale of *Intention for Passive Protection (IPP)* with Cronbach’s alpha of .66.

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, 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 .57.

Measure development for practice with online protections. Respondents rated six items (1 = strongly disagree to 5 = strongly agree) that paralleled Intention in online protection items. These items were worded towards the current online transactions practice such as buying, registering etc. and are self-reported by respondents. Cronbach’s alpha for the entire scale was .72. We also analyzed the underlying factor structure. From a factor analysis with Varimax rotation, two factors emerged.

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 .67.

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 .62.

Difference in Intention for Passive and Active Protection, and Passive and Active Protection Actions. In order to assess differences in the intentions for protection and actions for protection during online interactions between the U.S. and Indian sample, an analysis of variance was conducted. Analyses revealed that Americans report engaging in more intentions for passive protection ($M = 3.51$, $SD = .95$) and more passive protection actions ($M = 3.45$, $SD = .93$) 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. See Table 2.

	US <i>M (SD)</i> [†]	India <i>M (SD)</i>	
Intention for Passive Protection	3.51 (.95)	3.06 (.88)	$F(1, 792) = 44.27$ ***
Intention for Active Protection	3.56(1.00)	3.59 (1.06)	$F(1, 792) = .21$
Passive Protection Actions	3.45 (.93)	3.02 (.89)	$F(1, 794) = 39.68$ ***
Active Protection Actions	3.43 (.97)	3.33 (1.07)	$F(1, 794) = 1.61$

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

Table 2: Results of analyses of variance for Passive and Active Protection and Passive and Active Practice

Next, we analyzed the intercorrelations of two subscales of protection intentions and two subscale of protection actions in US and India (see Table 3). For the US and Indian samples, the intentions and the protective actions are significantly associated with one another. Notably, for the U.S. sample, the Intention for Passive Protection (IPP) and the Passive Protection Actions (PPA) are strongly associated. The relationship between Intention for Active Protection (IAP) and Active Protection Actions (APP) is the same. In the Indian sample, the relationship between Intentions and Actions is still statistically significant but is not as strong as in the U.S. sample.

	Intention for Passive Protection US (India)	Intention for Active Protection US (India)	Passive Protection Actions US (India)	Active Protection Actions US (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

Table 3: Inter-correlations of Intentions for Passive and Active Protection and Passive and Active Protection Actions in the U.S. and India

Predicting Intentions for Passive and Active Protection, and Passive and Active Protection Actions. In order to assess if willingness to disclose certain types of personal information predicts intention to engage in passive and active protection, and passive and active protective actions, a series of stepwise multiple regressions were conducted separately for the US and Indian samples. Analyses 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 for the U.S. sample. Analyses indicated that the linear combination of greater willingness to disclose email and less willingness to disclose medical information predicted active protection actions taken by the U.S. sample. Intention for active protection was best predicted by willingness to disclose email and less willingness to disclose financial information. See Table 4 for detail.

US		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*

Only the final model is presented. * p < .05, ** p < .01, *** p < .001.

Table 4: Combined regression tables for intentions for active and passive Protection and active and passive protection actions for the US sample

For the Indian sample, intention for active protection is predicted by willingness to disclose name, email address, media habits and less willingness to disclose credit information. For the Indian sample, intention for passive protection is predicted by willingness to disclose name and email and less willingness to disclose credit information and home address. Passive protection actions are best predicted by willingness to disclose name and home address. Active protection actions are best predicted by willingness to disclose name and email and less willingness to disclose credit information. See Table 5 for detail.

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**

Only the final model is presented. * $p < .05$, ** $p < .01$, *** $p < .001$.

Table 5: Combined regression tables for intentions for active and passive Protection and active and passive protection actions for the India sample

DISCUSSION, IMPLICATIONS, LIMITATIONS AND FUTURE RESEARCH

In both countries, consumers were more willing to disclose their media habits, name, email address, lifestyle and demographic information than other personal information. However, Indian consumers are more willing to disclose date of birth, work address and phone number, home phone number, medical history and financial history than the U.S. consumers. This suggests that there are significant differences in what personal information Indian and U.S. consumers are willing to disclose online and what they may perceive as making them vulnerable to adverse consequences as a result of the disclosure. This difference may be a due to cultural perspectives, different levels of Internet experience, or lack of awareness of the ramifications of divulging this type of information among other possibilities. Future research may be needed for specific factors.

Intention and actions for active protection, i.e., providing false information, frequently opting-out from marketing lists, and frequently deleting cookies from their computer, was relatively high across both nations with no significant differences. 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. consumer intending to and engaging in higher passive protection. These significant differences between the U.S. and Indian consumers regarding IPP and PPA suggests that American online consumers may be more cognizant of actions to take to ensure and protect their privacy, whereas Indian consumers may not be as sensitive to online privacy and security issues yet.

Based on our results, it appears 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. Companies that target Indian consumers may need to provide stronger security policies and measures to enhance consumer trust. That may encourage Indian consumer to be more willing to disclose their personal information online.

This study may help e-business companies understand consumers' attitude towards online privacy and security concerns. For global companies, it may mean that they cannot use the same policies and practices for all customers worldwide. Companies may need to tailor information gathering practices differently for customers in each cultural context, providing localized privacy policies. In addition, given the low scale of passive protection behavior in India, it implies the need for mechanisms to educate the consumers about privacy and security, so that they are more engaged in protecting their personal information.

In this study our findings are limited to the consumers representing the U.S. and India. The differences in cultures, regulations and laws related to online privacy and security, and hence, consumers' intentions and actions towards protection may vary across nations. A broader study that compares nations within each e-readiness index as well as across all three Tiers of e-readiness may provide more insight into privacy and security concerns. Future studies might explore factors that can moderate consumer's intentions and actions for passive and active protection.

REFERENCES

- Ackerman, E. (2009) FTC revises guidelines for online behavioral targeting, in *San Jose Mercury News*, February, 13, 2009, Available at http://www.mercurynews.com/business/ci_11690571?nclink_check=1.
- Ahuja, M., Gupta, B. and Raman, P. (2004) An Empirical Investigation of Online Consumer Purchasing Behavior. *Communications of the Association for Computing Machinery (CACM)*, 46,12ve, 145-151.
- Bellman, S., Johnson, E. J., Kobrin, S. J. and Lohse, G. L. (2004) International Differences in Information Privacy Concerns: A Global Survey of Consumers, *The Information Society*, 20, 313–324.
- Berinato S. and Scalet, S. (2006) The ABCs of Security. Available at <http://www.cio.com/security/> Retrieved February 10, 2008.
- Chin, W. W, Gopal, A., and Salisbury, W. D. (1997) Advancing the theory of adaptive structuration: The development of a scale to measure faithfulness of appropriation, *Information Systems Research*. 8, 4, 342-367.
- Cortada, J. W., Gupta, A. M. and Le Noir. M. (2007) How nations thrive in the Information Age: Leveraging information and communications technologies for national economic development, IBM Institute for Business Value study. Retrieved Feb 8, 2009 from <http://www-935.ibm.com/services/us/gbs/bus/pdf/g510-6575-01-infoage.pdf>.
- Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I. and Colautti, C. (2006) Internet Users' Privacy Concerns and Beliefs About Government Surveillance: An Exploratory Study of Differences Between Italy and the United States, *Journal of Global Information Management*, 14, 4, 57-93.
- Earp, J. B., and Baumer, D. (2003) Innovative web use to learn about user behavior and online privacy. *Communications of the ACM*, 46(4), 81–83 (April).
- Fair Information Practice Principles, Available at <http://www.ftc.gov/reports/privacy3/fairinfo.htm>. Retrieved February 1, 2009.
- Fusilier, M. and Durlabhji, S. (2005) An exploration of student internet use in India: the technology acceptance model and the theory of planned behavior, *Campus - Wide Information Systems*, 22, 4; 233-246.
- Gauzente, C. (2004) Web merchants' privacy and security statements: how reassuring are they for consumers? A two-sided approach, *Journal of Electronic Commerce Research*, 5, 3, 181-198.
- Han P. and Maclaurin, A. (2002) Do consumers really care about online privacy? *Marketing Management*, 11, 1, 35-38.
- Head M. & Yuan, Y. (2001) Privacy protection in electronic commerce – a theoretical framework, *Human Systems Management*, 20, 149–160.
- Hofstede, G. and Hofstede, G. J. (2004). *Cultures and Organizations: Software of the Mind*. New York: McGraw-Hill, U.S.A.
- Horrigan, J. B. (2008) Pew Internet and American Life Project, Pew Internet. <http://www.pewinternet.org/>.
- House, R. J., Hanges, P. J., Javidan, M., Dorfman, P. W., & Gupta, V. (2004). *Leadership, Culture, and Organizations: The GLOBE Study of 62 Societies*. Sage Publications, Inc.
- Internet World Statistics: Usage and Population Statistics (2009), Retrieved on Jan 15, 2009 from <http://www.internetworldstats.com/stats.htm>.
- Kelly, E. P. (2000) Ethical aspects of managing customer privacy in electronic commerce, *Human Systems Management*, 19, 4, 237-244.

- Kumaraguru, P., Cranor, L.F. and Newton, E. (2005) 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 - Sep 25.
- Liu, C., Marchewka, J. T. and Ku, C. (2004) American and Taiwanese perceptions concerning privacy, trust, and behavioral intentions in electronic commerce, *Journal of Global Information Management*, 12, 1, 18-40.
- Malhotra, N. K., Kim, S. S., and Agarwal, J. (2004) Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model, *Information Systems Research*, 15, 4, 336-355.
- Malhotra, N. K., Kim, S. S., and Patil, A. (2006) Common Method Variance in IS Research: A Comparison of Alternative Approaches and a Reanalysis of Past Research, *Management Science*, 52, 2, 1865-1883.
- Meinert, D. B., D. K. Peterson, J. R. Criswell and M. D. Crossland (2006). Privacy Policy Statements and Consumer Willingness to Provide Personal Information. *Journal of Electronic Commerce in Organizations*, 4, 1, 1-17.
- Milne, G. R., Rohm, A. J. and Bahl, S. (2004) Consumers' Protection of Online Privacy and Identity, *The Journal of Consumer Affairs*, 38, 2, 217-232.
- Painea, C., Reipsb, U., Stiegerc, S., Joinsona, A. and Buchanan, T. (2007) Internet users' perceptions of 'privacy concerns' and 'privacy actions'. *International J. Human-Computer Studies*, 65, 526-536.
- Park, C. and Jun, J. (2003) A cross-cultural comparison of Internet buying behavior: Effects of Internet usage, perceived risks, and innovativeness, *International Marketing Review*, 20, 5, 534-553.
- Phelps J., Nowak, G. and Farrell, E. (2000) Privacy Concerns and Consumer Willingness to Provide Information, *Journal of Public Policy and Marketing*, 19, 1, 27-41.
- Rudraswamy, V. & Vance, D. A. (2001) Transborder data flows: adoption and diffusion of protective legislation in the global electronic commerce environment, *Logistics Information Systems*, 14, 1&2, 127-136.
- Rust, R. T., P.K. Kannan, and N. Peng (2002) The Customer Economics of Internet Privacy, *Journal of the Academy of Marketing Science, MSI/JAMS Special Issue on Marketing to and Serving Customers on the Internet*, 30, 4, 451-460.
- Sheehan, K. M. and Hoy, M. G. (2000) Dimensions of Privacy Concern Among Online Consumers, *Journal of Public Policy and Marketing*, 19, 1, 62-93.
- Singh, N., Fassott, G., Zhao, H. and Boughton, P. D. (2006) A Cross-cultural analysis of German, Chinese and Indian consumers' perception of web site adaptation, *Journal of Consumer Behaviour*, 5, 1, 56-68.
- Son, J. and Kim, S. S. (2008) Information Privacy-Protective Responses, *MIS Quarterly*, 32, 3, 2008, 503-529.
- US Census Bureau News (2009), <http://www.census.gov/mrts/www/data/html/08Q4.html> Retrieved Feb 15, 2009.
- Warren S. and Brandeis, L. D. (1890) The right to privacy, Available at <http://louisville.edu/library/law/brandeis/privacy.html>. Accessed on November 10, 2006.
- Westin, A. F. (1967) *Privacy and Freedom*, Atheneum, New York.
- What is Privacy? (2004) Available at <http://www.rfidnews.org/library/2004/05/20/what-is-privacy/?issue=aHR0cDovL3d3dy5yZmlkbnV3cy5vcmcvbglicmFyeS8wMDI4NzQucGhwP2tleT0yNzE4>. Accessed on November 10, 2006.
- Zhang, X. (2005) What Do Consumers Really Know, *Communications of the Association for Computing Machinery (CACM)*, 48, 8, 44-48.