

# Demographic Characteristics and Concern for Information Privacy: An Empirical Study in the Context of Mobile Banking

Chien-Chih Chen<sup>1</sup>, Bireswar Dutta<sup>2</sup>, Mei-Hui Peng<sup>1,2</sup>

<sup>1</sup>Minghsin University of Science and Technology (MUST), Department of Information Management, Hsinchu, Taiwan, 304

<sup>2</sup>National Chiao Tung University, Institute of Information Management, Hsinchu, Taiwan, 300

<sup>2</sup>Corresponding Author

## ABSTRACT

This study investigates whether users have different privacy concerns regarding the information exchanging in m-banking according to gender, age, occupation, education, and mobile banking awareness. On the basis of the Concern for Information Privacy (CFIP) scale developed by Smith, Milburg, and Burke, in 1996, we carried out an online survey using 15 items in four dimensions, to examine mobile banking users' privacy concerns regarding the information exchanging in m-banking. The results recommend that the respondents had significant privacy concerns regarding m-banking and their educational level and mobile banking awareness significantly influenced their privacy concerns regarding unauthorized access and secondary use of information exchanging in m-banking. This study suggests that Indian government and banking authorities should organize comprehensive mobile banking awareness campaign, emphasizing on unauthorized access and secondary use of information exchanging in m-banking, to reduce people privacy concerns and facilitating the future implementation of m-banking.

**Keywords:** Concern for information privacy (CFIP); Mobile banking; Information exchanging; Demographic characteristics; Banking authority.

## 1. Introduction

One of the most significant developments over the last few decades was an increased organizational use of new technologies and banking sector is also taking part into it. Banking sector has been transforming from paper-based record keeping to digitalized record keeping process as part of ongoing efforts to cut down organizational and operational costs, saving time in order to keeping records and most importantly to improve customers' services. Information technology (IT), such as mobile banking (m-banking) is at the forefront of this ongoing transformation. As banking sector introduced m-banking services to conduct bank transactions, to administer accounts, to access customized information [1], to verify balances, transfer funds, pay bills, and perform various other transactions [2], the concern for information privacy (CFIP) began to escalate.

Concern for information privacy (CFIP) refers to individual's ability to control the terms under which their personal information is obtained and used [3]. Privacy concerns are identified globally, as the internet is a global medium, and allow the transmission of great amounts of customer information instantly across national borders [4]. Invasion of privacy on the internet involves the unauthorized collection, disclosure, or other use of personal information [5]. The interactive nature of the internet, which allows for two-way information exchanging between banking authorities and customers that improve commercial opportunities, introduces a unique environment in which privacy concern is heightened [6].

As m-banking continues to develop worldwide, banking authorities are collecting an escalating volume of personal information from customers and bring them together to generate detail profile of customers, in order to increase the efficiency and effectiveness of their operational strategies. So, it is practically impossible for customers to manage business online without providing personal information [7]. This information can then be sold and exchanged conceivably without the customers' permission, which increases customers' concerns as regards of having to expose personal information online, and regarding the manner in which such information might be used [8,9]. Such concerns extent from the intrusion of one's privacy to possible complexities resulting from online identity embezzlement. The

outcome from such concerns about privacy might choice from customers declining to provide personal information online to the absolute rejection of m-banking, or even minimizing the use of the internet [5,10].

Understanding how customers' CFIP or their concerns about how organizations exercise and protect their personal information [11], influence customers' perception to conduct online dealings is significant to our knowledge for customer-oriented m-banking. For example, if CFIP has a significant direct influence on perception to take part in online processes, both researchers and practitioners may wish to understand how to improve some of these concerns for direct influences. In contrast, if CFIP only influences on perception to conduct through other factors, then efforts could be directed at influencing those factors through both CFIP along with through their additional antecedents. In order to meet the requirements, Smith et al. [11] developed and endorsed an instrument that recognizes and measures the primary dimensions of individuals' concerns about organizational information privacy practices. Additionally, Stewart and Segars [12] examined the factor structure of the CFIP instrument and found that CFIP may be more stingily represented as a higher-order factor structure instead of a correlated set of first-order factors. These two studies made an effort to validate measurements of CFIP in an organizational context and recommended that CFIP is possibly influenced by customers' characteristics, but neither of the study suggested a theoretical foundation for such study.

Despite the numerous advantages of m-banking and increased rate of adoption by banking sector, the actual adoption rate by individual is still quite low [13]. Several studies have shown that CFIP is the greatest barrier to its adoption [10,14,15,16,17,18]. As, individuals' personal and financial information are reasonably more sensitive than other kinds of information [6, 19]. Therefore, individuals typically have considerable concerns regarding the privacy of such information [20].

To better deal with these privacy issues, the factors affecting on individual's privacy concerns must be understood. Although previous studies on m-banking have examined customer willingness to conduct has focused primarily on the role of trust and trustworthiness either applying trust theory or applying acceptance, and adoption-based theories for example frameworks from which to study trust. The researches based on trust theories have a tendency to focus on the structure of trust or on antecedents of trust [21,22]. Adoption-and acceptance-based researches consist of studies used Technology Acceptance Model [23] and diffusion theory [24] to investigate the influences of trust within well-established models. Among the influential factors, researchers have the most interest in customer characteristics, such as age, gender, and educational level [25]. Though, the outcomes reported in studies concerning the influence of customer characteristics on privacy concerns remain conflicting and inconclusive [25,26]. So, the influence of people's characteristics on their information privacy concerns needs to be reviewed to improve our current understanding of this issue.

To explore individual's concerns regarding m-banking privacy, we conduct a preliminary investigation of the differing characteristics of various Indian groups and their m-banking privacy concerns. Specially, this study investigates the influence of m-banking users' age, gender, occupation, educational level, and mobile banking awareness on their privacy concerns regarding m-banking because, even though individuals typically have superior online privacy concerns [6], they are more possibly to seek personal and financial information online. We believe that the results of this study can improve our current understanding of m-banking privacy concerns, which allow both the government and banking authorities to initiate better privacy policies and personal information collection and processing practices.

## **2. Literature review**

### **2.1 Mobile Banking in India**

Mobile banking (m-banking) can be considered as "actions that result in an entity's right to use to the sort of banking activities (associated with savings or credit) by using mobile devices such as cell phones" [27]. Based on the circumstances, this might also incorporate mobile payments [28]. In developed countries, the keen development of smartphones and other mobile devices has brought about the significant diffusion of mobile banking. According KPMG [29] the total number of mobile banking users surpasses 0.8 billion globally and is projected to hit 1.8 billion by 2019. During the last few years, mobile banking has generated a deluge in banking industries in developing countries such as India through the escalated use of smartphones [30]. Thus, highest rates of adoption of mobile banking in the world have been seen in India and China [29].

Indian banks have been offering m-banking services since 2009 as a means to give their customers, especially those in rural areas, seamless access to banking services [31]. The main advantage of m-banking is that the people in remote area can also access the banking services at ease. According to KPMG [29], India ranks fifth in the world regarding its rate of adoption of m-banking services that currently surpasses 50%. In recent years, Indian m-banking has reflected a growing trend (even if in low volume). According to report by Reserve Bank of India [32], during 2015-16, the value of transactions through prepaid payment instruments (PPI) cards and mobile-wallets increased to 254 billion Indian Rupees (INR) and 206 billion (INR) respectively, against 105 billion (INR) and 82 billion (INR) respectively in the

previous year. But m-banking still has a long way to go as majority of customers prefer banking in the traditional ways [33]. An important question here is why customers are not adopting mobile banking as per assessment.

Researchers frequently have been studied about the barriers and drivers of m-banking adoption to improve understanding of why customers do not adopt m-banking [34]. According to RBI [35] report, two potential challenges were identified to attaining m-banking piercing to the predictable level. The first challenge is regarding the enrollment process for example mobile number registration, the m-pin (mobile personal identification number) generation procedure, privacy and security concerns, and training for both bank staff and customer. The second challenge is more regarding technical concerns (access networks for transactions, complicated transaction processes, and does not coordinate between mobile network operators and bank authorities to let customers a composed experience). Other issues regarding lack of awareness among customers. Additionally, the transaction procedures is unwieldy and involves numerous authentication input from customers. Table 1 indicates a review of several barriers of m-banking adoption.

**Table 1.** Studies represent the barriers of m-banking adoption.

Barriers	Sources
Privacy and Security concerns	36,37,38,39
Lack of knowledge (awareness)	38,40,41,42
Relative advantages	43,44
Lack of easy-of-use	38,43,45, 47
Lack of usefulness (traditional banking services)	38,46,47
Subjective norm	43,48

From the data in Table 1, we can understand that main barriers to the adoption of m-banking are related to concerns about privacy and security, lack of awareness and difficulty of use. Though, the investment from government and banking sector in building technological infrastructure has eradicated a number of technological barriers. Nonetheless, barriers such as privacy and security concerns and perceived risk are still persisting. Several studies on online banking adoption [49,50,51] have discussed about significant influence of privacy and security risk regarding adoption. They concluded that concern of the lack of privacy and security are significant barriers to the adoption of online banking [38].

### **2.2 Privacy, Information privacy, and concerns regarding Information privacy**

Warren & Brandies [52] defined the need to protect people's rights in their landmark article The Right to Privacy. Privacy refers to a person's ability to control the access others have to their personal information [3]. Privacy is violated when people cannot control their communication with social and physical environments [19]. A person's privacy is determined by the sociopolitical system and economic development of the society they live in [3]. But, privacy concerns are not a recent phenomenon; they frequently arise when the public perceives a threat from new information technologies that develop the surveillance, storage, retrieval, and communication of personal information [19]. Moreover, great numbers of mobile banking service providers have developed technical standards as well as organizational and legal frameworks that promise the highest level of privacy and security possible.

With the intense advancement of information technologies, the sharing and exchanging of information has become more convenient and easier. The people's concerns regarding the privacy of personal information have increased [3] because a considerable amount of personal information is exchanged, stored, and shared. In the field of marketing, information privacy concerns have been referred as an obstacle to customers' adoption of online commerce [53], their purchasing behavior [54], and their willingness to reveal personal information online [25]. In the same way, privacy concern regarding information exchanging becomes a barrier to m-banking promotion. Specifically, the information processed by m-banking authorities is individuals' sensitive personal and financial data, which are directly related to their personal and economical privacy. Therefore, privacy protection is crucial for m-banking context. Though most professionals understand the necessity for confidentiality, a detailed knowledge and responsibility to protect privacy is lacking. So, this study explores information privacy issues related to the collection, storage, use, and information exchanging on m-banking context.

### **2.3 Prior CFIP Research**

A 15-item instrument hereafter referred to as the CFIP instrument was developed by Smith et al., [11] as a way of measuring and identifying the multi-dimensional nature of consumer CFIP. The outcome was an ungenerous 15-item instrument that contains four dimensions of the Concern for Information Privacy (CFIP) scale: collection, secondary use, unauthorized access, and errors. This instrument recommends that people with considerable information privacy concerns perceive that (1) excessive data is collected; (2) personal information is used for undisclosed purposes; (3) personal information is not sufficiently protected from unauthorized access; and (4) most of the data is inaccurate [11]. Stewart and Segars [12] further tested these four dimensions. Therefore, the four dimensions identified by Smith et

al.,[11]seem to provide a complete framework for information privacy concerns and have been extensivelyreferred[12,24].

#### **2.4 Demographics and CFIP**

Abundant previous researches indicated that, numerous factors can affect people's privacy concern. As Phelps et al. [55]explored that customers' privacy concerns were determined by four factors: (1) the types of personal information are requested; (2) how the information control is offered; (3) What are the potential consequences and benefits are offered in the exchanging; and (4) customer characteristics. Among these influencing factors, researchers are most interested in customer characteristics, for example age, gender, and educational level [25].

Concerning age, the results of previous studies observe that a person's age can affect their privacy concerns [25]. For instance, young people naturally take more risks. Additionally, they have fewer privacy concerns because they are young, generally less wealthy, and have not yet established a reputation; as a result, they have less to lose [56]. According to study by Bellman et al. [57] and Sheehan [58]older Internet users are generally more concerned about online information privacy. They have a greater desire to control the amount of information collected about them as well as a greater need to have their names removed from mailing lists [59].Moreover, the study by Graeff and Harmon[60] found that older Internet users are also more sensitive to privacy issues. Phelps et al. [55]performed a direct marketing shopping survey and verified that age is not associated to information privacy concerns. Milne and Rohm [59]studiedeven if people read the privacy protection policies of companies, and the result showed that age was positively interrelated with whether a person read privacy protection policies. According to the results by Jandaand Fair [61]also presented that age was positively interrelated with the privacy concerns with regard to the internet.

Concerning gender, several studies have confirmedthat gender differences in online privacy concerns and consequent privacy protection behavior[26,58]. Laric et al. [62]found statistically significant effects based on gender. In general, womenperceive more online risk and report higher privacy concerns compared to men.The results of thestudy by FogelandNehmad [26]pointed out that women were more concerned with information privacy compared to men.Women were also comparativelyreluctant to discuss their personal information on the internet. Yet, thoughmen had a more interest in the internet and better computer skills compared to women, gender was not related to information privacy concerns [63]. According to the study by JandaandFair [61]women and men are different significantly on the subject of their internet privacy concerns and obtained that women had more internet privacy concerns compared to men. However, Chen et al. [63]showedin their study that gender was not correlated with the information privacy concerns of people without online shopping experience. The study results by Phelps et al. [55]regardingthe direct marketing shopping investigation also discovered that gender was not related to information privacy concerns. Milne and Rohm[59]investigatedif people read the privacy protection policies of companies and their study results showed that men hardly ever read these policies.

Concerning educational level, a person's education is usually considered being positively correlated to their financial status [56]. In other words, the higher education people obtain, the greater the chance of them to be economically successful. Therefore, educated people may putmore emphasis on privacy protection. A well-educated person may be well knowledgeableas regard privacy issues and better understanding of the circumstances. Though, betterunderstanding of information privacy may affect people's privacy concerns [56]. For example, the results of the study by Phelps et al. [55]about direct marketing shopping showed that educational levels and information privacy concerns were not related. Milne and Rohm[59] investigatedin their study of whether people read the privacy protection policies of companies and noticed that people's educational level was negatively interrelated with their reading of privacy protection policies.

So, a review of related studies points out that our consideration of the relationship between information privacy concerns and demographics remains indecisive. Moreover, due to the specialty of the m-bankingenvironment, this study further investigates the influence of occupations and mobile bankingawareness on information privacy concerns. These two features were seldom discussed in previous studies. So, we consider that these featuresrequire further clarification, particularly in m-banking perspective.

### **3. Materialsand methods**

#### **3.1 Questionnaires**

This study references the CFIP scale developed by Smith et al. [11] and recommends indicators for measuring users' privacy concerns under information exchanging context. Privacy concerns were measured by five-point Likert scale items that were taken from the measurement of CFIP outlined in Smith et al. [11]: collection (four items), unauthorized access (three items), secondary use (four items), and errors (four items). To improve the reliability and validity of the indicators, this study modified the content of the items regarding information exchanging inm-banking and obtained a preliminary version of the indicators. Six experts, that is, threeprofessors in MIS field, two doctoral scholars in the online bankingsector, and one doctoral scholar in the information management field, were invited to review the

indicators and adapt the meaning of the items in the four dimensions. Next, nine people, that is, two persons with a senior high school certificate, two persons with a bachelor's degree, two person with a master degree, two retired persons, and one housewife, were invited to undergo a pretest. On the basis of the suggestions obtained following the pretest, we modified and finalized the final version of the indicators. The content of the 15 items is shown in Table 2.

**Table 2.** Indicators for concerns regarding information exchanging inm-banking.

Dimension	Item
Collection	It usually bothers me when bank authorities ask me for personal information.
	I sometimes think for a while when bank authorities ask me to provide personal information.
	It bothers me to give personal information to so many bank authorities.
	It bothers me that bank authorities collect too much personal information.
Unauthorized Access	Bank authorities should devote more time and efforts to preventing the unauthorized access of individual' personal information.
	Bank authorities should prevent unauthorized people from accessing individual' personal information without considering the cost.
	Bank authorities should take more measures to ensure that unauthorized people cannot use their computer to access individual' personal information.
Secondary Use	Bank authorities should never use individual' personal information for any other purposes, unless it has been authorized by the individual.
	When people give personal information to bank authoritiesfor some reason, the bank authority should never use the information for any other purpose.
	Bank authorities should never sell individual' personal information to other banks.
	Bank authorities should not share individual' personal information with other banks unless it has been authorized by the individual.
Error	Bank authorities should repeatedly check the accuracy of individual' personal information without considering cost.
	Bank authorities should use more procedures to ensure the accuracy of individual' personal information.
	Bank authorities should have a more comprehensive procedure to correct for errors in individual' personal information.
	Bank authorities should devote more time and manpower to verify the accuracy of individual' personal information.

### **3.2 Participants and Procedures**

Due tousers' perceptions of several privacy features are not comprehended[64], this studycould be considered investigative by nature. Cooper and Schindler[65]insisted that convenience sampling is a useful approach during the early stages of investigative study. Therefore, this study used a convenience sampling approach to conduct the survey. The questionnaires were presented on a web site. Previous study done by Angst and Agarwal [66] has recommended that the survey participants ought to be familiar with the research context. Thus, to generate more traffic to the website, subjects were informed of the survey via e-mail and encourage them to complete a questionnaire on the web site. Additionally, subjects were encouraged to forward the survey e-mail to people interested in privacy issues related to m-banking. To prevent duplicate responses, the online survey stored the respondents' IP address and multiple responses from the same IP address were excluded. Because the respondents of this study participated online, the research population was difficult to confirm. In other words, the response rate was not easily calculated.

The questionnaire was used for this study comprised three sections. In the first section (cover page), the purpose of the survey and a definition of m-bankingand information exchangingwere provided. The second section of the study instrument was designed to get basic information about respondents', including their age, gender, educational level, occupation, and awareness of mobile banking. The third section contained indicators of concern for information exchanging(15 items). The respondents were instructed to use a five-point Likert scale to evaluate each item (1 for strongly disagree and 5 for strongly agree).

## **4. Results**

### **4.1 Descriptive Statistics**

This study collected 297 questionnaires. Of which fifteen of the responses were considered unusable, either incomplete or from the same IP address; the final analysis included 282 responses. The demographic background of the survey

respondents is shown in Table 3. The results in Table 3 point out that the respondents differed regarding gender, age, educational level, occupation, and mobile banking awareness.

Table 3. Survey respondents' demographics.

Type	Sub-type	Count	Percentage (%)
Gender	Male	187	66.31
	Female	95	33.69
Age	<=30	137	48.58
	31-40	31	10.99
	41-50	61	21.63
	>=51	53	18.79
Education Level	High School or under	56	19.85
	College	94	33.33
	Master or above	132	46.80
Occupation	Public Sector	40	14.18
	Private Sector	242	85.81
Mobile Banking Awareness	Have not heard	38	13.47
	Have heard, but not understand	100	35.46
	Understand	144	51.06

Table 4 shows the descriptive statistics of the constructs, including the four dimensions and 15 items. Using the five point Likert scale, item mean values which exceed 3 point out that people have information privacy concerns. The mean value of the collection item is 3.61, which points out that people have certain concerns regarding bank authorities collecting their personal information. Nevertheless, the mean values of the three other dimensions, which all exceeded 4, point out that people are extremely concerned about secondary uses, unauthorized access, and errors regarding information exchanging onm-banking. Generally, people have serious privacy concerns regarding their information exchanging inm-banking.

**Table 4.** Factor loading, mean, S.D., Cronbach's alpha of the privacy concerns items.

Dimension	Items	Loadings	Mean	S.D.	Cronbach's Alpha
Collection (Mean =3.61 SD =0.781)	Col1	0.833	3.38	0.986	0.864
	Col2	0.786	3.67	0.878	
	Col3	0.836	3.66	0.944	
	Col4	0.837	3.74	0.976	
Unauthorized Access (Mean =4.45 SD =0.638)	UA1	0.831	4.46	0.784	0.693
	UA2	0.742	4.32	0.965	
	UA3	0.823	4.58	0.676	
Secondary Use (Mean =4.67 SD =0.518)	SU1	0.884	4.65	0.615	0.847
	SU2	0.852	4.72	0.672	
	SU3	0.815	4.75	0.567	
	SU4	0.748	4.57	0.718	
Errors (Mean =4.27 SD =0.846)	ER1	0.746	3.94	0.976	0.857
	ER2	0.897	4.46	0.757	
	ER3	0.857	4.42	0.788	
	ER4	0.862	4.27	0.854	

**4.2 Reliability and Validity**

Regarding the respondent analysis, Cronbach’s  $\alpha$  for the four dimension variables all exceeded 0.7, except for the variable “unauthorized access” (0.693). Because of the exploratory nature of this study, a Cronbach’s  $\alpha$  higher than 0.5 indicates sufficient reliability [67]. Consequently, to determine whether the question items possessed sufficient discriminant validity and convergent validity, we employed factor analysis. We found that the factor loading value for all items exceeded 0.7 (Table 4), representing that the questionnaire had satisfactory validity [68].

**4.3 Demographic Characteristics and Privacy Concern for Information Exchanging inm-banking**

To explore the effect of people’s demographic characteristics on their privacy concern for information exchanging, *t*-test, analysis of variance (ANOVA), and Scheffe’s post-hoc techniques were employed to determine whether the respondents’ age, gender, occupation, educational level, and mobile bankingawareness cause differences in their privacy concern for information exchanging.

**4.4 Effect of Gender, Age, and Occupations**

The *t*-test and results of ANOVA pointed out that people’s m-banking privacy concerns in the four dimensions, that is to say, collection, unauthorized access, secondary use, and errors, were similar irrespective of their gender, age, and occupation (Tables 5, 6, and 7).

**Table 5.** *t*-test for privacy concern of information exchanging between gender (*N*=282).

Dimension	Gender				<i>t</i>	<i>p</i> -value
	M ( <i>N</i> =187)		F ( <i>N</i> =95)			
	Mean	SD	Mean	SD		
Collection	3.46	0.872	3.65	0.716	-1.046	0.317
Unauthorized Access	4.43	0.684	4.51	0.575	-0.815	0.434
Secondary Use	4.53	0.576	4.75	0.517	-1.166	0.296
Errors	4.17	0.837	4.35	0.768	-0.173	0.892

**Table 6.** Differences in privacy concern of information exchanging on age (*N*=282).

Dimension	Mean				<i>F</i>	<i>p</i> -value
	A(<=30)	B(31–40)	C(41–50)	D(>=51)		
Collection	3.51	4.35	4.58	4.16	0.647	0.576
Unauthorized Access	3.46	4.47	4.65	4.38	0.881	0.455
Secondary Use	3.68	4.54	4.64	4.14	0.612	0.613
Errors	3.57	4.35	4.57	4.18	0.974	0.414

**Table 7.** *t*-test for privacy concern of information exchanging between occupations (*N*=282).

Dimension	Occupations				<i>t</i>	<i>p</i> -value
	Public Sector ( <i>N</i> =40)		Private Sector ( <i>N</i> =242)			
	Mean	SD	Mean	SD		
Collection	3.54	0.774	3.57	0.796	-0.417	0.617
Unauthorized Access	4.43	0.526	4.45	0.647	-0.515	0.616
Secondary Use	4.65	0.337	4.63	0.534	-1.457	0.154
Errors	4.14	0.753	4.17	0.827	-0.017	0.987

**4.5 Effect of educational level**

The ANOVA results indicate that people with different educational levels have differing concerns regarding unauthorized access and secondary uses of their privacy concern for information exchanging inm-banking. Results of the Scheffe’s post-hoc analysis indicated that people with a master degree have more concerns regarding the secondary use and unauthorized access of their information exchanging inm-banking compared to people who had only a high school (or lower) education. Additionally, people with a college degree showed more concern regarding unauthorized access compared to people with a high school (or lower) education. (Table 8).

**Table 8.** Differences in privacy concern means of information exchanging on educational level (N=282).

Dimension	Educational level					
	A (N=56)	B(N=94)	C(N=132)	F	p-value	Scheffe test
Collection	3.52	3.50	3.56	0.051	0.951	
Unauthorized Access	4.13	4.38	4.58	5.752	0.005	C>A
Secondary Use	4.38	4.57	4.71	8.876	0.000	C>A, B>A
Errors	3.86	4.09	4.19	1.997	1.40	

**Note:** A: High School or under; B: College; C: Master or above

**4.6 Effect of mobile banking awareness**

The ANOVA results point out that people’s awareness of mobile banking influence their privacy concerns as regards unauthorized access and secondary use; though, it has no influence on m-banking collection and errors (Table 9). Moreover, the results of Scheffe’s post-hoc analysis indicated that people who had heard of or understood about information exchanging of m-banking had greater concerns regarding secondary use and unauthorized access (Table 9).

Table 9. Differences in privacy concern of information exchanging on mobile banking awareness (N=282).

Dimension	Mobile banking awareness					
	A (N=38)	B(N=100)	C(N=144)	F	p-value	Scheffe test
Collection	3.50	3.56	3.62	0.052	0.954	
Unauthorized Access	4.10	4.37	4.57	5.754	0.004	C>A
Secondary Use	4.31	4.62	4.73	8.875	0.000	C>A, B>A
Errors	3.84	4.10	4.20	1.998	0.142	

**Note:** A: Have not heard; B: Have heard, but not understand; C: Understand

**5. Discussion**

The findings of this study point out that gender is not significantly correlated with privacy concerns regarding information exchanging in m-banking, which is in agreement with the findings of previous studies [55,56]. People share inclusive information to bank authority to receive better services. Though, the results indicate that, regardless of gender, people expect their personal information to be sufficiently protected by the bank authority. For instance, men typically want to protect information related to personal and financial, contact information such as email address, telephone number, name of the preferred bank, from which they received better services and women wish to prevent others from viewing their detail financial history, contact information, personal detail like marital status. Therefore, both women and men value the privacy of their personal information. This explains why gender does not significantly affect people’s privacy concerns regarding information exchanging in m-banking.

Concerning age, the results of this study point out that age is not significantly correlated with information privacy concerns related to m-banking, which supports the results of previous studies [55,62]. Regarding m-banking, personal information is extremely important for bank authorities when dealing and providing services to customer. However, personal information is a vital reference. To receive better services, customers of varying ages should provide bank authorities with comprehensive information too. Though, they should be concerned with how bank authorities protect and use their information. This may explain why age does not have a significant effect on people’s information privacy concerns regarding information exchanging in m-banking.

Regarding educational level, the results of this study point out that people’s educational level was significantly correlated with their information privacy concerns regarding m-banking, which are in agreement with the results of previous studies [56,64]. The post-hoc analysis of this study points out that highly educated respondents are more concerned regarding with the privacy of information exchanging in m-banking, particularly regarding unauthorized access and secondary use. To further develop information exchanging in m-banking, multiple dimensions, including

laws and regulations, operational mechanisms, and information and communication technologies must also be considered.

However, the findings of this study endorse that occupation is not significantly correlated with people's privacy concerns regarding information exchanging regarding m-banking. This finding is consistent with the finding of previous studies [56,64]. Since mobile banking is relatively new and constantly changing area of business management and information technology, people recognize that they must need to provide personal and financial information while performing through mobile banking system and this information will be processed by the bank authorities when treating the customers. Most people in India have a certain level of awareness of information exchanging on mobile banking; thus, occupation does not influence people's privacy concerns regarding information exchanging on mobile banking.

Finally, the results indicated a significant correlation exists between mobile banking awareness and people's privacy concerns regarding information exchanging in m-banking. The post-hoc analysis results also point out that people have greater privacy concerns regarding m-banking when they are more familiar with m-banking, mostly regarding unauthorized access and secondary use. People with a greater understanding of m-banking better understand the risks and challenges of information exchanging in m-banking and have greater privacy concerns regarding m-banking, specifically regarding unauthorized access and secondary use of information exchanging in m-banking.

## **6. Conclusion and Implications**

This study examined the differences between users' characteristics and privacy concerns of information exchanging regarding m-banking. The study findings confirm that user's educational level and mobile banking awareness are significantly correlated with their privacy concerns regarding unauthorized access and secondary use of information exchanging in m-banking. Though, this study did not find any significant correlation between user's gender, age, occupation and their privacy concerns regarding m-banking. The study findings point out that highly educated users have greater information privacy concerns related to information exchanging in m-banking, especially the unauthorized access and secondary use of their personal information. In addition, users who are familiar with m-banking have superior information privacy concerns associated with information exchanging in m-banking, particularly regarding unauthorized access and secondary use. The implications of study findings for academicians and practitioners are discussed below.

### **6.1 Managerial Implications**

Overall, the results of this study indicate that users have reasonably significant privacy concerns regarding information exchanging in m-banking. Hence, we propose that the government should employ various types of media (for example TV, radio, newspapers, and leaflets) [69], mainly those of Internet channels (such as e-mails, blogs, and virtual communities) [70,71], to promote mobile banking awareness, increase banking users' understanding of m-banking, and reduce their privacy concerns. We also recommend that bank authorities should promote consumer awareness and develop an m-banking system according to regulations that is subsequently audited and certified by the government. Additionally, to reduce users' concerns regarding unauthorized access of their information in m-banking, bank authorities should develop an information security management mechanism that follows to international standards. Indian Government has introduced the Information Technology Act, 2000 [72] deals with contractual aspects of use of electronic records. Indian laws mandate that bank authorities do not share or exchange customers' information regarding m-banking with external units or use customers' personal information for any other purpose without the customer's written consent. If users' concerns regarding secondary use of their information regarding m-banking can be reduced, they can step by step accept the implementation of m-banking.

Regarding highly educated people and people with better m-banking knowledge, we suggest that the government and bank authorities provide a comprehensive explanation of exchanging information regarding m-banking. A comprehensive introduction of information exchanging regarding m-banking should include the techniques, potential risks, and measures implemented to protect information from unauthorized access and incorrect application. This should improve users' understanding of m-banking, thereby increasing their trust and reducing their privacy concerns regarding m-banking. Generally, highly educated people are believed to hold greater social influence [73,74]. Thus, once they understand and accept m-banking and trust that bank authorities provide adequate privacy protection for information exchanging, they can act as advocates of m-banking. However, these people can use their social influence to promote m-banking, which benefits the implementation of m-banking in the future.

Nonetheless, we consider our work offers the foundation for an alternative justification for technology adoption in m-banking perspective. Specially, demographic characteristics might also impact on technology adoption, though our study recommends that this impact is mediated by CFIP. It could be interesting to make a decision if there is empirical support for this proposition. In fact, if these factors are associated as per we have suggested, then we can improve our better understanding of technology adoption. For instance, instead of depending only on principles that have

traditionally been used to justify adoption with a focus on potential advantages, there might be principles that could explain technology adoption with a focus on individuals' balanced personality towards privacy. In other words, it is likely to possible that future technology adoption decisions will be less determined by usefulness factors but more by concerns that go against human nature or principles [75]. Comparing which of these factors suggests an exciting influence is missing to future research. Though, we would not be astonished if demographic characteristics have a colossal impact in highly personalized technology scenario than in less personalized scenario, for example a working atmosphere with fixed technologies like personalized recommendation engines in m-banking.

It is important to realize that privacy has always been inversely proportional to functionality. However, the more personalized a technology is, it is more likely depend on personalized individual's information. But an increased enquiry for extremely personal information is also potentially linked to intensification of individual's threat perception and related with the desire to be protected from maltreatment. The rationale to be protected is an integral part of human nature, and consequently part of the psychological personality too. Study by Black (Black, 2006) even claimed that threat perceptions and the urge to be protected is biologically motivated and can be traced back to human evolution [76].

This study can be considered as an initial step towards understanding the psychological state of individuals regarding adoption of technology and how it influences on individuals' concerns for privacy in the m-banking perspective. In comparison to Sheehan [58], who developed a typology of Internet users and segmented them into fundamentalists, rationalists, and indifferent individuals based on their CFIP, the findings of current study could be used to segment individuals based on the pattern of particular personal demographic characteristics. Despite the fact that demographic characteristics could not be changed as they are inherent personalities that are found to be constant over time [77], knowing that certain demographic characteristics are important in the development of CFIP can be used as a leverage point for m-banking researchers and technology designers in a similar way.

Current study presents some linkages between demographic characteristics of individuals and their behavioral intentions that can be regarded as predominant societal traits or more especially as personality characteristics of target groups. Either way, this would provide information that might be helpful to develop approaches to shift behavioral intentions of individuals by bringing down concerns for information privacy.

For example, understanding the behavioral characteristics of individual could help m-banking providers in developing a relationship between itself and customers by displaying their awareness of these concerns. One of the greatest opportunities m-banking providers have in reaching customers is providing a formal privacy policy. It has been confirmed that a formal and clear privacy statement put forth a positive impact on individuals' attitude; hence, m-banking providers could form their privacy policy more efficiently by reshuffling it to deal with the issues of each demographic characteristic type. For instance, they may want to allure to the intellectual feature of individuals while picking up the wording and details of their privacy policy. Individuals may possibly be more sensitive to incomplete policy statements that do not fully concentrate on the fair information practice principles. Regrettably, it has been determined that a significant number of m-banking service providers do not provide adequate information regarding privacy policies to address all the practical principles [78]. M-banking service providers should look into this gap in privacy policy practice sincerely as it is a great opportunity to alleviate individuals' concerns by developing their privacy policy statement to address all key areas of privacy concerns.

If demographic characteristics are inert to modifications, then other non-demographic-associated factors are most possibly to moderate their impact on CFIP. A pattern of such moderating factors might be circumstantial or situational indications that could act together with some of the characteristics and that could trigger them to be more significant in certain contexts [79]. Suppose, for instance, technology designers can propose m-banking that matches the individuality of a highly coconscious person? Designers must have to confirm that they concentrate on an individual's need for structure and meticulousness to the degree that technology is competent of sustaining a guaranteed-based communication and in consequence moderating personal concerns. On the other hand, a reverse strategy can be put into effect when such kinds of concerns are minimized. For instance, highly educated individuals could be sensitized to privacy by presenting them with technology that warns them towards integral privacy threats. Generally, we look forward to moderators in the relationship between demographic characteristics and CFIP could be principally technology-specific. Though, this could be kept left for future researchers to validate empirically.

## **6.2 Theoretical Implications**

Prior studies pointed out the relationship between people's demographics and information privacy concerns [56,61,63] in several contexts. However, least number of researches has been conducted in the m-banking perspective, that is, user's information privacy concerns regarding m-banking. This dearth of attention to the relationship in the m-banking perspective is challenging because it can significantly influence the promotion of m-banking in the future.

For this study, we conducted a preliminary investigation of users' privacy concerns regarding information exchanging in m-banking. We found that users place significant importance on the unauthorized access and secondary use of their information exchanging. Therefore, the results of this study can offer a foundation for a detailed understanding of how user's concerns for information exchanging regarding m-banking can be reduced. Additionally, we believe that future privacy studies inspect the crucial role information privacy concerns have in shaping user's attitudes toward m-banking.

The most of the studies regarding m-banking privacy concerns have concentrated on what banking authorities or trustees would offer and how they could function to improve users' trust to reduce their privacy concern. But these factors are considered as an extrinsic to users or trustors, who visits banking websites. However, there is dearth of researches on the intrinsic factors that might impact on any recognized situation concerning privacy concern of banking operational systems. However, previous researches have already showed that privacy concern did influence on individuals ways of disclosing personal information and using the websites [80], but different individuals could be influenced more or less to information breaches due to individuals' different perception regarding privacy. So, individuals privacy concern towards banking operational systems more or less is a significant addition to the study, has previously not really differentiated among demographics characteristics. Therefore, the principal contribution of this study is identifying users' characteristics as the intrinsic factors influencing on online privacy concern particularly in m-banking perspective. This is new and presents the privacy theory with a dual perspective for users' privacy concern antecedents from both intrinsic and extrinsic aspect. Therefore, privacy concern is not only about the consideration of users and their behaviors, as previous researches have studied, but depends also on users' intrinsic characteristics and situations in terms of their demographic characteristics.

For this study, we conducted a preliminary investigation of how Indian individuals' different demographic characteristics influence on their privacy concerns regarding m-banking. We found that Indian individuals irrespective of their demographic characteristics place substantial importance on the privacy issues regarding secondary use and unauthorized access of information. Therefore, the findings of this study can offer a foundation for a detailed consideration of how individual's information concerns regarding m-banking could be lowered.

Considering the dimensions of personality, while the reason why some personality or demographic characteristics influence on privacy concern and others do not is still a vulnerable question. The findings of study do support the need to include demographic characteristics in the privacy concern analysis of disclosing information regarding m-banking information exchange. The same applies to awareness regarding technology, especially mobile banking awareness in our study, which, as other aspect of personal dispositions, play important and significant roles in increasing the disutility of disclosing demographic information in m-banking information exchange. This indicates the requirement to include awareness information as a special type of personal private information and to fit in situation-specific experiences in the study of effectiveness and ineffectiveness enhancers.

## **7. Contributions**

This article contributes to the information privacy literature by providing a conceptualization of a broader perspective of information privacy exchange regarding m-banking context, improving the predictability of concern for information privacy (CFIP), and empirically validating how CFIP may control individuals' provision of personal information during the function of mobile commerce. Regarding practical contribution, this study empirically examined the relationship between user's demographics and their privacy concerns regarding information exchanging in m-banking. The results indicate that people's educational level and mobile banking awareness is correlated with their privacy concerns regarding information exchanging in m-banking. Thus, government and bank authorities should emphasis on these findings and develop better privacy protection policies for m-banking to reduce user's privacy concerns regarding information exchanging. From a theoretical perspective, this study enriches to CFIP literature by further investigating the relationship between users' characteristics and information privacy concerns. Furthermore, this study empirically validated the suitability of utilizing the CFIP instrument in m-banking environment. In addition, because the number of bank have risen, demographic studies on consumers' view of information privacy have become increasingly essential. This study fills this research gap.

## **8. Limitation and Future Research**

First, the participants were recruited using an online questionnaire in a comparatively limited time, which may influence on the representativeness of the results. Therefore, more diverse participants should be included in future studies. For example, obtaining participants from online environment settings who are more likely to be candidates of using of m-banking may provide interesting insights in future studies. In fact, differences of personal characteristics are one of potential factors for differences in privacy concerns as individuals differ demographically and culturally. Moving forward, research must be conducted across different cultural perspectives and slowly evolve from the individual perception of study towards group perspective which could identify the influences of peer pressure and group norms.

Future study should address the cumulative impact of different personality characteristics, with each characteristic reciprocally working together to make a more nicety psychological profile of an individual and their inception of concern for information privacy. Additionally, the participants' responses to the online self-report questionnaire may have been influenced by their perception of the questionnaire items, resulting in common method bias. So, researchers should consider using comprehensive interviews and case study methods in the future.

### References

- [1] Tiwari, R., & Buse, S. (2007). *The Mobile Commerce Prospects: A Strategic Analysis of Opportunities in the Banking Sector*. Hamburg University Press.
- [2] Gefen, D., Straub, D., & Boudreau, M. (2000). Structural equation modeling techniques and regression: Guidelines for research practice. *Communications of AIS*, 4(7), 2–76.
- [3] Westin, A.F. (1967). *Privacy and Freedom*. New York, Atheneum Press.
- [4] Nijhawan, D.R. (2003). The Emperor Has No Clothes: A Critique of Applying the European Union Approach to Privacy Regulation in the United States. *Vanderbilt Law Review*, 56(3), 939-976.
- [5] Wills, C.E. & Zeljkovic, M. (2011). A Personalized Approach to Web Privacy: Awareness, Attitudes, and Actions. *Information Management & Computer Science*, 19(1), 53-73.
- [6] Sheehan, K.B. & Hoy, M.G. (2000). Dimensions of privacy concern among online consumers. *Journal of Public Policy & Marketing*, 19(1), 62–73.
- [7] Rust, R.T., Kannan, P.K. & Peng, N. (2002). The Customer Economics of Internet Privacy. *Journal of the Academy of Marketing Science*, 30(4), 455-464.
- [8] Ohm, P. (2010). Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. *UCLA Law Review*, 57, 1701-1777.
- [9] Yao, M.Z., Rice, R.E. & Wallis, K. (2007). Predicting User Concerns About Online Privacy. *Journal of the American Society for Information Science and Technology*, 58(5), 710-722.
- [10] Dinev, T. & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, 17(1), 61–80.
- [11] Smith, H.J., Milburg, S.J. & Burke, S.J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly*, 20(2), 167–196.
- [12] Stewart, K.A. & Segars, A.H. (2002). An empirical examination of the concern for information privacy instrument. *Information Systems Research*, 13(1), 36–49.
- [13] Funk, J. L. (2009). The emerging value network in the mobile phone industry: The case of Japan and its implications for the rest of the world. *Telecommunications Policy*, 33, 4–18.
- [14] Culnan, M.J. & Armstrong, P. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science*, 10(1), 104–115.
- [15] Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I. & Colautti, C. (2006a). Internet users' privacy concerns and beliefs about government surveillance. *Journal of Global Information Management*, 14(4), 57–93.
- [16] Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I. & Colautti, C. (2006b). Privacy calculus model in e-commerce – a study of Italy and the United States. *European Journal of Information Systems*, 15(4), 389–402.
- [17] Hwang, H.G., Han, H.E., Kuo, K.M. & Liu, C.F. (2012). The Differing Privacy Concerns Regarding Exchanging Electronic Medical Records of Internet Users in Taiwan. *J Med System*, 36, 3783–3793.
- [18] Alkhalifah, A. & Amro, S.A. (2017). Understanding the Effect of Privacy Concerns on User Adoption of Identity Management Systems. *Journal of Computers*, 12(2).
- [19] Culnan, M.J. (1993). How did they get my name—an exploratory investigation of consumer attitudes toward secondary information use. *MIS Quarterly*, 17(3), 341–361.
- [20] McGraw, D., Dempsey, J. X., Harris, L. & Goldman, J. (2009). Privacy as an enabler, not an impediment: Building trust into health information exchange. *Health Aff.* 28, 416–427.
- [21] Bhattacharjee, A. (2002). Individual trust in online firms: scale development and initial test. *Journal of Management Information Systems*, 19(1), 211-241.
- [22] Gefen, D.E. (2000). E-commerce: the role of familiarity and trust. *Omega*, 28, 725-737.
- [23] Gefen, D. & Straub, D.W. (2000). The relative importance of perceived ease of use in IS adoption: A study of e-commerce adoption. *Journal of the Association for Information Systems*, 1(8).
- [24] Van Slyke, C., Belanger, F. & Comunale, C. (2004). Factors influencing the adoption of Web-based shopping: The impact of trust. *Database for Advances in Information Systems*, 35(2), 32-49.
- [25] Li, H., Sarathy, R. & Xu, H. (2011). The role of affect and cognition on online consumers' decision to disclose personal information to unfamiliar online vendors. *Decision Support System*, 51, 434–445.

- [26] Fogel, J. & Nehmad, E. (2009). Internet social network communities: Risk taking, trust, and privacy concerns. *Comput Human Behav*, 25, 153–160.
- [27] Porteous, D. (2007). Just how transformational is m-banking? Commissioned by Finmark, [http://www.finmarktrust.org.za/accessfrontier/Documents/transformational\\_mbanking](http://www.finmarktrust.org.za/accessfrontier/Documents/transformational_mbanking).
- [28] Mishra, V. & Singh Bisht, S. (2013). Mobile banking in a developing economy: A customer-centric model for policy formulation. *Telecommunications Policy*, 37(6), 503–514.
- [29] KPMG. (2015). <https://www.kpmg.com/UK/en/IssuesAndInsights/ArticlesPublications/Documents/PDF/mobile-banking-report-2015.pdf>.
- [30] Business-standard (2014). [http://www.business-standard.com/article/finance/mobile-banking-zooms-as-india-getssmarter-114081100826\\_1.html](http://www.business-standard.com/article/finance/mobile-banking-zooms-as-india-getssmarter-114081100826_1.html)
- [31] Gupta, S., Yun, H., Xu, H. & Kim, H.W. (2017). An exploratory study on mobile banking adoption in Indian metropolitan and urban areas: a scenario-based experiment, *Information Technology for Development*, 23(1), 127–152.
- [32] RBI report. (2016). <https://rbidocs.rbi.org.in/rdocs/Publications/PDFs/0FRTP16A120A29D260148E58B484D4A60E381BB.PDF>.
- [33] Wang, Y., Wang, Y., Lin, H., & Tang, T. (2003). Determinants of user acceptance of internet Banking: an empirical study. *International Journal of Bank Marketing*, 14(5), 501-519.
- [34] Bamoriya, D. & Singh, P. (2012). Mobile banking in India: Barriers in adoption and service preferences. *Journal of Management*, 5(1), 1–7.
- [35] RBI report, 2014. <https://www.rbi.org.in/scripts/PublicationReportDetails.aspx?UrlPage=&ID=760>.
- [36] Hayikader, S., Hadi, F.N.H. & Ibrahim, J. (2016). Issues and Security Measures of Mobile Banking Apps. *International Journal of Scientific and Research Publications*, 6(1).
- [37] Reaves, B., Scaife, N. & Bates, A. (2015). Mo (bile) Money, Mo (bile) Problems: Analysis of Branchless Banking Applications in the Developing World, *Proceedings of the 24th USENIX Security Symposium*.
- [38] Safeena, R., Date, H., Kammani, A. & Hundewale, N. (2012). Technology Adoption and Indian Consumers: Study on Mobile Banking. *International Journal of Computer Theory and Engineering*, 4(6), 1020–1024.
- [39] Filiol, E. & Irolla, P. (2015). (In) Security of Mobile Banking....and of Other Mobile Apps. *Black Hat Asia*.
- [40] Luvanda, A., Kimani, S., & Kimwele, M. (2014). Lack of Awareness by End Users on Security Issues Affecting Mobile Banking: A case study of Kenyan Mobile Phone End Users. *Journal of Information Engineering and Applications*, 4(5).
- [41] Thyagarajan, G. (2015). Mobile Banking – A Review. *International Journal of Management and Social Science Research Review*, 1(14).
- [42] Tiwari, A.K., Agarwal, R. & Goyal, S. (2014). Imperative & challenges of mobile banking in India. *International Journal of Computer Science & Engineering Technology*, 5(03).
- [43] Puschel, J., Mazzon, J. A. & Hernandez, J. M. C. (2010). Mobile banking: Proposition of an integrated adoption intention framework. *International Journal of Bank Marketing*, 28(5), 389-409.
- [44] Brown, I., Zaheeda, C., Douglas, D., & Stroebel, S. (2003). Cell phone banking: predictors of adoption in South Africa – an exploratory study. *International Journal of Information Management*, 23, 381-394.
- [45] Koenig-Lewis, N., Palmer, A., & Moll, A. (2010). Predicting young consumers’ take up of mobile banking services. *International Journal of Banking Marketing*, 28(5), 410-432.
- [46] Riquelme, H. & Rios, R.E. (2010). The moderating effect of gender in the adoption of mobile banking. *International Journal of Bank Marketing*, 28(5), 328-341.
- [47] Dasgupta, S., Paul, R., & Fuloria, S. (2011). Factors affecting behavioral intentions towards mobile banking usage: Empirical evidence from India. *Romanian Journal of Marketing*, 3(1), 6-28.
- [48] Sripalawat, J., Thongmak, M. & Ngramyarn, A. (2011). M-banking in metropolitan Bangkok and a comparison with other countries. *The Journal of Computer Information Systems*, 51(3), 67-76.
- [49] Chen, Y. H. & Barnes, S. (2007). Initial trust and online buyer behaviour. *Industrial Management & Data Systems*, 107(1), 21–36.
- [50] Hernandez, J. M. C. & Mazzon, J.A. (2007). Adoption of Internet banking: Proposition and implementation of an integrated methodology approach. *International Journal of Bank Marketing*, 25(2), 72– 88.
- [51] Howcroft, B., Hamilton, R. & Hewer, P. (2002). Consumer attitude and the usage and adoption of home-based banking in the United Kingdom. *International Journal of Bank Marketing*, 20(3), 111–121.
- [52] Warren, S.D. & Brandeis, L.D. (1890). The right to privacy. *Harvard Law Review*, 4(5), 193–220.
- [53] Zorotheos, A., & Kafeza, E. (2009). Users’ perceptions on privacy and their intention to transact online: a study on Greek internet users. *Direct Marketing*, 3(2), 139–153.

- [54] Tsai, J.Y., Egelman, S., Cranor, L. & Acquisti, A. (2011). The effect of online privacy information on purchasing behavior: An experimental study. *Information Systems Research*, 22(2), 254–268.
- [55] Phelps, J.E., D'Souza, G. & Nowak, G.J. (2001). Antecedents and consequences of consumer privacy concerns: An empirical investigation. *Journal of Interactive Marketing*, 15(4), 2–17.
- [56] Chen, J., Yue, Z. & Heath, R. (2001). An exploratory investigation of the relationships between consumer characteristics and information privacy. *Marketing Management Journal*, 11, 73–81.
- [57] Bellman, S., Johnson, E.J., Kobrin, S.J. & Lohse, G.L. (2004). International differences in information privacy concerns: A global survey of consumers. *Information Society*, 20(5), 313–324.
- [58] Sheehan, K. (2002). Toward a typology of internet users and online privacy concerns. *The Information Society*, 18, 21–32.
- [59] Milne, G. R. & Rohm, A. J. (2000). Consumer privacy and name removal across direct marketing channels: Exploring opt-in and opt-out alternatives. *Journal of Public Policy & Marketing*, 19(2), 238–249.
- [60] Graeff, T. R. & Harmon, S. (2002). Collecting and using personal data: Consumers' awareness and concerns. *Journal of Consumer Marketing*, 19(4/5), 302–318.
- [61] Janda, S. & Fair, L.L. (2004). Exploring consumer concerns related to the internet. *Journal of Internet Commerce*, 3(1), 1–21.
- [62] M.V. Laric, D.A. Pitta, and L.P. Katsanis, Consumer concerns for healthcare information privacy: a comparison of US and Canadian perspectives. *Research in Healthcare Financial Management*, vol. 12, no. 1, pp. 93–111, 2009.
- [63] Chen, K., Alan, I. & Rea, J. (2004). Protecting personal information online: A survey of user privacy concerns and control techniques. *Journal of Computer Information System*, 44(4), 85–92.
- [64] Milne, G.R. and Culnan, M.J. (2004). Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices. *Journal of Interactive Marketing*, [Volume 18, Issue 3](#).
- [65] Cooper, D.R. & Schindler, P.S. (2001). Business research methods (Seventh edition). *Irwin/McGraw-Hill*, New York, 192.
- [66] Angst, C.M., & Agarwal, R. (2009). Adoption of electronic health records in the presence of privacy concerns: The elaboration likelihood model and individual persuasion. *MIS Quarterly*, 33(2), 339–370.
- [67] Nunnally, J.C. (1967). *Psychometric theory (First edition)*. New York, *McGraw-Hill*, 226.
- [68] Straub, D., Boudreau, M.C. & Gefen, D. (2004). Validation guidelines for IS positivist research. *Communications of the Association for Information Systems*, 13, 380–427.
- [69] Tee, E.S. (2011). Development and promotion of Malaysian dietary guidelines. *Asia Pacific Journal of Clinical Nutrition*, 20(3), 455–461.
- [70] Bonfadelli, H. (2002). The internet and knowledge gaps: A theoretical and empirical investigation. *European Journal of Communication*, 17(1), 65–84.
- [71] Howard, P.E.N., Rainie, L. & Jones, S. (2001). Days and nights on the internet—the impact of a diffusing technology. *American Behavioral Scientist*, 45(3), 382–404.
- [72] IT Act, (2000). <http://meity.gov.in/content/information-technology-act-2000>.
- [73] Hollingshead, A.B. (2011). Four factor index of social status. *Yale Journal of Sociology*, 8, 21–52.
- [74] Meyer, J.W. (1977). The effects of education as an institution. *American Journal Sociology*, 83(1), 55–77.
- [75] Myers, M.D. & Miller, L. (1996). Ethical dilemmas in the use of information technology: an aristotelian perspective. *Ethics & Behavior*, 6(2), 153–160.
- [76] Buss D.M. (2005). (Ed.) *The Handbook of Evolutionary Psychology*. John Wiley & Sons, Hoboken, NJ.
- [77] McCrae, R.R., Costa, P.T., Hrebickova, M., Urbaneck, T., Martin, T.A., Oryol, V.E., Rukavishnikov, A.A. & Senin, I.G. (2004). Age differences in personality traits across cultures: self-report and observer perspectives. *European Journal of Personality*, 18, 143–157.
- [78] Ryker, R., Lafleur, E., McManis, B. & Cox, K.C. (2002). Online privacy policies: An assessment of the fortune E-50. *Journal of Computer Information Systems*, 42(4), 15–20.
- [79] Tett, R.P. & Burnett, D.D. (2003). A personality trait-based interactionist model of job performance. *Journal of Applied Psychology*, 88(3), 500–517.
- [80] Tsoi, H.K. & Chen, L. (2011). From Privacy Concern to Uses of Social Network Sites: A Cultural Comparison via User Survey, IEEE International Conference on Privacy, Security, Risk, and Trust, and IEEE International Conference on Social Computing.