Paper:

Hossain, M. & Dwivedi, Y. (2014). What improves citizens' privacy perceptions toward RFID technology? A cross-country investigation using mixed method approach. *International Journal of Information Management, 34*(6), 711-719.

http://dx.doi.org/10.1016/j.ijinfomgt.2014.07.002

What improves citizens' privacy perceptions toward RFID technology? A cross-country investigation using mixed method approach

Mohammad Alamgir Hossain
School of Business, North South University
Block B, Bashundhara R/A
Dhaka, BANGLADESH
Tel: +880-(0)2-8852000 extension 1778
Email: mahripon@yahoo.com

Yogesh K Dwivedi
School of Management
Haldane Building
Swansea University
Singleton Park, SA2 8PP, UK
Tel: +44(0)1792602340
Email: ykdwivedi@gmail.com

ABSTRACT

Privacy is a serious concern to Radio Frequency Identification (RFID) technology. Several companies worldwide scrapped RFID projects because of high resistance from the consumers and their advocacy groups – which actually demand RFID-specific privacy policies. This concern is even more acute when RFID is used in public applications; because, in general case, citizens cannot refuse to provide data, and the data collected by a government agency would offer a serious threat if are shared among third parties. Limited research has been performed in this specific issue; they all agree that perceived privacy increased RFID acceptance. But, what drives privacy perceptions are yet to be researched - this study closes this research gap. In order to conduct the current research, the mixed method of research approach has been adopted. In the qualitative research stage, the authors conducted two focused-group discussions and eight in-depth interviews in two different countries: Australia and Bangladesh; arguing that the status, and the perceptions and tolerance of the citizens on privacy are different in these two regions. The explored factors have been examined with empirical data obtained from these two countries. It is found that, there are distinct differences in perceptions in developed and developing countries. The detail findings offer practical suggestions to the agency managers so that they can ensure better privacy of the citizens. As a significant theoretical contribution, this study enhances the existing literature identifying the antecedents of privacy which play even different roles in different cultural backgrounds.

Keywords – RFID; privacy; public use; mixed method; Australia; Bangladesh

1. Introduction

In ancient times, slaves would collect data and/or information about citizens/subordinates for their masters; now, technology replaces the slaves but perform even better (Cas, 2005). However, government convinces its people that, identifying a person uniquely is essential for a country, and using a technology would produce a better society, in terms of security and public facilities. Currently, many countries have developed and implemented radio frequency identification (RFID)-based human identification system; national identity (ID) cards and electronic passports (e-passport) are the main as the tools to combating potential terrorism activities and crimes. Moreover, although often far from realistic nature, the personal information which it captures would enhance the service quality of the State e.g. quick and accurate disbursement of funds (Can 2005). Unfortunately, some (corrupted) officials sometimes consider personal data as 'commodity' and expose/sell them to third-party (marketing) companies – which is a complete violation of *information privacy*.

Information privacy refers to users' rights "to keep information about themselves from being disclosed to others" (Rognehaugh, 1999, p. 125). Maintaining information privacy in the current world with ubiquitous technologies is very a complex task (Cas, 2005). For instance, in a library RFID technology can develop a profile answering who have used the book, for how long, and so on (Dwivedi, Kapoor, Williams, & Williams, 2013). Hence, the use of RFID in national systems where citizens' data is captured creates a significant debate on the users' privacy (Fosso Wamba, Anand, & Carter, 2013; Thornley, Ferguson, Weckert, & Gibb, 2011). Actually, the basic and fundamental discomfort comes from using RFID technology is related to its capability to identify an object uniquely, record real-time and spatial information, and linking the information with other (unauthorised) business (Thiesse, 2007). By using ubiquitous technologies, more personal data are now harvested and exposed, in terms of quality and quantity; however, less effort is observed on privacy protection (Can 2005).

The extent of behavioural literature on privacy are actually invested their effort to examine the effect of privacy toward people's acceptance of a specific technology (e.g. Hossain & Prybutok, 2008)and on privacy protection techniques. Still, 'satisfactory' results are not clear (Sutanto, Palme, Tan, & Phang, 2013) which could present RFID as "privacy-friendly" (Langheinrich, 2009). Actually, the actual problem (and hence the potential solution) lies somewhere else. The critics of the technology acceptance model (TAM) often argue that, every manager knows that *perceived usefulness* and *ease of use* would drive people to accept a technology, but what are the drivers of these two constructs are actually more important. Similarly, there is a huge literature gap that explores the antecedents of *perceived privacy* of the users and examines their relative effect. Here, *perceived privacy* is defined as the degree to which a citizen of a given society believes that s/he has the right to control the collection and use of her/his personal information, even after s/he disclosed it to others (Hossain & Prybutok, 2008). Therefore, the main objective of this study is to explore the catalysts of perceived privacy taking RFID as a representative technology and applying in national applications.

Furthermore, this study has been conducted in Australia and Bangladesh realizing that people's view on privacy differs in culture. Prior studies found that RFID-perceptions vary in locations (e.g. Leimeister, Leimeister, Knebel, & Krcmar, 2009). Thiesse (2007) believe that, "the difference between the valuation of privacy in Western and Asian cultures.... could play a much more important role than expected" (p. 227). Comparing between the people of Hong Kong and Canada, Bailey and Caidi (2005) found that, difference in cultural notions of privacy may affect the acceptance of innovations in information and communication technologies. Similarly, Sareen (2005) established that, citizens from Indian, where privacy gets lower priority, put personal privacy as the highest priority to their financial transactions. Acknowledging the necessity of examining privacy in different cultural settings, this study puts a unique effort conducting a field study as well as a survey in Australia and Bangladesh applying same interview protocol and survey questionnaire, respectively.

2. Background

Radio Frequency Identification (RFID) is an automated data-capturing and data-storing technology. The captured data can be used to identify an object uniquely (RFID-Journal, 2005). RFID privacy issues is well explored in literature; however, the researchers are concerned and concentrated mainly in retail stores item-level tagging (Brown & Russell, 2007a) and privacy issues of the customers - emphasizing technical and technological issues (e.g. Chong & Chan, 2012; Juels, 2006; Kelly & Erickson, 2005; Peslak, 2005). It should be noted that, unlike the use of RFID in retail stores where a proper and practical implementation of RFID system does not affect individual customers' privacy (Murray, 2003), securing the privacy of the citizens is more sensitive and complex (Hossain & Prybutok, 2008; Peslak, 2005). First of all, the customers enjoy all the luxury to reject some technologies (e.g. mobile phones, ATM cards or Internet) or reject shopping from an RFID-enabled shop that may affect their privacy (Gilbert & Shim, 2003) (Masnick, 2003). However, many public applications of RFID technology such as e-passport do not leave any substitute option; hence, people cannot refuse the technology, and may have little or no choice whether to provide personal information (Cullen & Reilly, 2008). The more sensitive part is, the applications are not 'closed' but necessarily interconnected. For example, the amount of 'family assistance' is decided by the income and number of child(ren); therefore, the data captured from tax office or the hospitals have to be shared by the associated government agency. Hence, the captured personal data about the citizens is accessed, handled and shared by many departments or authorities. The proposed (but failed) national identity card of Australia "intended that thirteen Government agencies would use the *Australian Card*" (Jordan, 2010). Consequently, the issue of citizens' privacy comes as very prominent and thus demands a special attention from the deploying authorities to keep the data confidential and inaccessible to any unauthorized use (Kelly & Erickson, 2005). But, several privacy leaking through data-abuse incidents such as supplying the citizens' information to marketing companies (particularly with Malaysia's MyKad) have raised and/or strengthened public concern and perception protecting privacy with highest priority. Hence, this current study addresses a sensitive and timely issue of privacy, in the context of RFID use in a much focused area – national applications – which is actually scarcely researched.

National identity card (e-ID) is the main application of RFID technology in public applications. Malaysia is the first country that introduced RFID-based national identity card (MyKad) in 2001 (Thomas, 2004). Several other nations including Hong Kong, Estonia, Finland, Belgium, Portugal, Spain, China, and Albania issued e-ID to its citizen. The next major application of RFID in national use is the electronic passport (e-passport). In both cases, an RFID chip is integrated in the card/passport which stores personal data (e.g. name, date of birth, address) as well as biometrics (e.g. facial, fingerprint, and iris recognition of the bearer) (Juels, Molnar, & Wagner, 2005). Many countries already have implemented e-passports while many others are in the process. Again, Malaysia is the forerunner that issued e-passport in 1998 which is followed by "approximately 95 countries ... including all G8 nations" (Baird, 2012, p. 8; Kowlessar, 2012). In fact, there is a continuous global and regional pressure on the adoption of RFID in passports and identity cards. The International Civil Aviation Organization (ICAO) has mandated for every traveller with RFID-enabled electronic passport (e-passport) by April 2014; however, the deadline has been extended to 2017 (Kowlessar, 2012). Similarly, as a regional pressure, European Union (EU) is on its way to implement an RFID-based globally unique cross identification system with the intention of sharing the ID with allied countries for the purposes like Interpol investigations or visa-free-entry. That means, RFID is becoming a necessity than a choice for the citizens of a country.

Privacy has been considered as the most important building block of ubiquitous technologies including RFID (Cas, 2005). An RFID-consumer survey conducted by Capgemini (2005) revealed that 'privacy' is perceived as the top concern; similar is observed with other ubiquitous technologies as well such as Smart Phones (Sutanto et al., 2013). The nature and level of privacy intrusion actually come from both the capability of collecting (personal) information, and more importantly, because of the easy share of the information. As the government-agencies put (an implicit) mandate to its people to use RFID technology, it has to take the most responsibilities to secure privacy of the people.

This section focuses on the issue if there is any difference on RFID privacy – government *vs.* private use. The treaty of the European Union states that, everyone's privacy right "shall be no interference by a public authority…except … is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime and freedoms of others'' (Coblentz & Warshaw, 1956). Almost similar provisions are made in the U.S. and other countries too (Directive, 1995). Therefore, collecting and using citizens' data through RFID by the state-applications is lawfully justified. Hence, consumer advocates do not object the government use of RFID for national interest (CASPIAN, 2003), but urge and demand that under no circumstance users' personal and sensitive information should not be abused. In general, *personal information* means any information (a) relating directly or indirectly to a living individual; (b) from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and (c) in a form in which access to or processing of the data is practicable (Hong-Kong-Government, 2012). And *sensitive information* means personal data that reveals "racial and ethnic origin, political opinions, religious, philosophical or moral beliefs, labour union membership, and information concerning health conditions or sexual habits or behaviour" (Argentine-Government, 2008). Hence, the information that is stored by the government agencies through e-IDs is *personal* and *sensitive*. Therefore, even for national interest, citizens' information has to be authentically accessed by the right personnel and lawfully used for national interest – that means, even to a government, the information privacy is not waived. Unlike the customers who are reluctant to be tracked, the people are willing to sacrifice their privacy right for citizenship gain till of its authorized use (Cas, 2005). What is missing, however, is a convincing trade-off between the users' expectation and degree of managing those expectations by the respective agencies; that means, what citizens believe as the tools of securing their privacy, and whether that are offered and managed by the government, at least to an acceptable level. Whenever people talk about 'privacy', researchers tend to find out the technologies solutions which may be effective but are not sufficient; the behavioural approach also has to be considered with even more efforts/importance.

Irrespective of developing or developed countries, and in public or private sector, there are always some debates and lack of trust for using a strong technology like RFID which have the capability of tracking a person in real-time. Still, privacy is a big concern especially in developed countries, whereas people from developing countries are bit flexible, especially to a government. Unlike a developed country, in many developing countries including Bangladesh, the constitutional bodies are not beyond the control of the government. For instance, the election commission in Australia is the sole authority that conducts every related activities to an election; however, this is not necessarily a practical truth in Bangladesh – here, a political government may use citizens' data for their benefits such as political harassments to opposition parties or manipulate the election result (Akhtar, 2001). Moreover, discrimination on the basis of religion, political orientation, past criminal record or medical history is also very prominent, which is even be made easier with e-ID and hence a potential source of privacy abuse cases (Thomas, 2004). Still, the people are less sensitive to privacy; sometime they even feel good to be personally recognized, even if it breaches his/her privacy rights. Moreover, they be grateful for having a service even though it is his/her right, and usually do not bother how are they treated (by the government agencies) rather what they got at the end. Consequently, generally speaking, a Bangladeshi possess higher personal tolerance and place lower importance and high sacrifice on personal privacy – the things are just opposite in Australia (Ohkubo, Suzuki, & Kinoshita, 2005). For instance, in 1985 the Hawke Government proposed for a national system of identification, which was rejected in the 1988 referendum (Saunders, 2008). Again in 2006, (although claimed not as the national identity card), Howard Government proposed a 'smart card' "that would fight welfare cheats, terrorism" but "the scheme failed so quickly" and could not get that much success (Saunders, 2008). In both occasions, the main concern was the 'privacy'. On the contrary, most of the Asian countries including Bangladesh have been experiencing national identity card for generations; and people here are believed to be more resilient on privacy.

3. Methodology

Epistemologically, positivism approach that is found to have dominating role in IS research is considered for this study (Y. Dwivedi, 2008). Driven by the objective and the nature of the study, within positivist paradigm, the mixed-method approach has been adopted which is actually a combination of qualitative and quantitative methods. "The mixed method approach is appropriate as RFID research is still in its infancy [stage]"; hence, "a combination of methodological techniques assists in exploring the RFID adoption phenomenon more fully" (Brown & Russell, 2007b, p.252). First, a semi-structured question was developed from the existing literature which was employed during conducting the qualitative study. The qualitative field study explored and/or confirmed and/or contextualized the factors, and developed an initial research model; the model has been validated with quantitative data obtained from a survey.

In the first stage, qualitative data were obtained from two focus group discussions (FGD) and eight in-depth interviews conducted with RFID users in Perth (Western Australia), and Dhaka (Bangladesh). FGDs were conducted one in each city, consisting six and seven discussants in Perth and Dhaka, respectively – each having around 70 minutes. In addition, eight direct interviews (four in Perth and four in Dhaka) were conducted to explore users' insights on this current research agenda. The participants have been using at least one RFID application provided by the State; SmartRider in Perth and SPASS in Dhaka – both are the ticketing cards for public transport commuting service.

4. Findings of the qualitative study and developing the research model

At the beginning of each the FGD and the interviews, the participants were given a brief outline of the RFID technology and the research purpose. The respondents were allowed to discuss on the privacy issues related with RFID technology, and were probed when required. To start the discussion, the following questions were asked:

a. What is your perception on privacy, related to RFID technology use?
b. What features you perceive as useful to maintain privacy on RFID data?

The Organization for Economic Cooperation and Development (OECD) prepared a guideline for privacy protection that developed eight principles including collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability. However, OECD guideline is not updated "for almost a quarter of century" which actually demand some contemporary approaches. The current study explored the guidelines and validated with empirical data, which is actually not contradictory but complimentary to the OECD principles; yet more generalized and perception-based. The following sections present the findings of the qualitative study, get support from the extent literature, and propose the hypotheses, while developing the dimensions of each concept (i.e. construct).

4.1 Explicit consent

The respondents from both sample perceive that, explicit consent from the citizen is essential for securing privacy; the clear consent must state that the "data would not be used in a manner other than it mean to be", and the data owner-should sign the consent form or check the box in digital form. In literature, Cas (2005) proposed that, an "informed consent" should be obtained from the users that also would request the user for permission to collect, use and share the data. The 'collection limitation principle' of OECD guideline too refers to the awareness and informed consent of the people whose data are being collected (Cas, 2005). However, associated agencies may use the data without further consent, but, "It is not automatic to waive the privacy for every agency" when only one agency is granted the permission".

While collecting personal data, two methods are practiced by the agencies: *opt out* (where the citizens' information may be distributed till they refuse to do so) and *opt in* (personal information cannot be shared till the permission is granted by the citizens) (Laudon & Laudon, 2012). Karjoth and Moskowitz (2005) found that, most of the privacy solutions are dependent on *opt-out* method, but, the *opt-in* choice can provide better result (Culnan & Bies, 2003). Similar observation is noted by the respondents who suspect that, government agencies abuse the *opt-out* model of data acquisition-and-use; they demand a quick shift to *opt-in* model. Collectively, the explicit consent is believed to have a positive effect increasing the privacy perceptions of the citizens; hence, the first hypothesis is developed as follows incur:

Hypothesis 1 Explicit consent will increase users' confidence regarding privacy issues.

4.2 Detail privacy statement

The filed study emphasized that, while collecting data, the agencies should publish and provide a detail privacy statement. When asked about what the things the respondents expect to see on the privacy statement, the following items come up as significant: the purpose of data collection, how the data will be collected and used, how long the data will be kept and the security policy of acquired data (i.e. security measures). The findings are in line with the prior literature (e.g. Eckfeldt, 2005; Floerkemeier, Schneider, & Langheinrich, 2005). Moreover, the 'purpose specification principle' of OECD guideline suggests for declaring the purpose and usage definition of data acquisition; similarly, the 'use limitation' emphasizes on not disclosure or transfer of the acquired data (Cas, 2005).

The respondents from Bangladesh found that such detail statement is very rare and therefore develop ambiguity and lack of confidence on government's use of citizens' data. As far Australia sample is concerned, detail privacy statement is provided to the citizens, at least in theory, because of serious privacy concern of the citizens (Cas, 2005). Regardless, both samples claim that the detail statement would increase the confidence of the citizens toward securing their privacy. Therefore, the next hypothesis becomes:

Hypothesis 2 Detail privacy statement in personal data collection forms will increase users' confidence regarding privacy issues.

4.3 Legislative protection

Government (through its official statutory, and administrative processes) is one of the most powerful sources, if not the most, of ensuring its citizens' privacy (Thiesse, 2007); hence, regulatory restrictions are necessary (Cas, 2005). The respondents re-establish that, every country should have legislations against unauthorized access and/or use of personal data, harvested by government agencies. "Under no circumstance the State should tolerate any information-abuse" collected from an RFID system; "lack of legislation is one of the main reasons for privacy abuse with RFID in Malaysia". They also mentioned that, although some existing privacy laws cover the use of data collected by electronic systems, more direct laws are to be considered dealing with the issues particular to RFID (Thiesse, 2007). "Governments should behave smartly with handling a smart technology" – hence, they appreciate and recommends contemporary law such as the *E-Government Act 2002* of United Sates of America which provides a framework for the agencies to follow assessing the impact on privacy when implementing RFID-like technologies in particular. Literature too is in favour; proposing a four-step process of privacy 'maintenance', Cas (2005) proposed for developing "new regulatory fundaments of privacy where old ones are becoming insufficient" (p. 26).

The Australian respondents believe that legislation against privacy abuse can secure their privacy; in the worst case, they can go to court and ask for compensation. On the contrary, the Bangladeshi respondents claim that, there is no such legislation in Bangladesh which can protect privacy of the citizens - while the movement has just has been initiated (Farjana, 2012). Even so, the respondents are sceptical about the effectiveness of such law because, in general, the practice of laws is very insignificant; however, legislative protection should be in place, regardless. Hence, it is proposed that:

Hypothesis 3 Legislative protection will increase the perceived privacy of the citizens.

4.4 Data-owners' accessibility

From a consumer perception study, Günther and Spiekermann (2005) found that ''regardless of privacy enhancing technology employed, consumers feel helpless toward the RFID environment, viewing the network as ultimately more powerful than they can ever be''. As a solution, Thiesse (2007) proposed the RFID vendors to put more effort on user control on data and data security technologies. The respondents of the field study believe that, to their personal data, citizens must have a control over the amount of access of the data that the government agencies have. They discussants believe that citizens, once they have duly evidenced their identity, should have the right to request obtaining the data and requesting to change the information on their personal data-field.

Data owners' accessibility also secure currency and accuracy of data with low costs – in line with the data quality principle of OECD (Cas, 2005). This would empower the users too. The Bangladeshi respondents claim that, unfortunately, people do not have sufficient access on their data; upgrading profile data "*involves unnecessary hassle – both financial as well as mental".* Therefore, they are. On the contrary, the Australian respondents believe that the access on their personal data is more easy, and to modify. Yet, they demand that, instead of updating data on different agencies, a central information system would be more effective, which would be accessible and checkable by the users. Therefore, the fourth proposition is developed as follows:

Hypothesis 4 Data owners' accessibility will increase users' confidence regarding privacy issues.

4.5 Data authenticity

To ensure privacy, it is a fundamental requirement that data should be safeguarded properly using privacy enhancing technologies. Additionally, "specially equipped and trained teams" should work on data preservation who also will "detect violation of data protection regulations" (Can 2005, p. 25). It is commonly observed especially in developing countries that data is not technologically secured enough, and hence is a soft target by hackers. More often, citizens' data are sold to marketing organizations and hence violating privacy of the citizens. Therefore, the respondents urge that the systems require government-owned and government-managed central cryptographically-secured database, without sharing the information to third-party. Respective agency must take technical and organizational measures to guarantee the security and confidentiality of personal data in order to avoid their alteration, loss, and unauthorized consultation or treatment. Moreover, they emphasized that, more importantly, as techniques evolve every now and then the agencies should upgrade data authenticity with contemporary measures as well, not just relying on the past techniques. Another useful means of securing privacy is to anonymisze or pseudonymize the data (Cas, 2005). The discussants agreed that, developing countries have less effective data-authenticity mechanism than that in developed countries; yet, developed countries need to adopt contemporary mechanisms that are effective to combat with hackers. Hence, the next proposition can be stated as follows:

Hypothesis 5 Data authenticity will increase users' confidence regarding privacy issues.

4.6 Communication channels

Finally, it is found from the analysis that, the role of *communication channels* is very important to secure the privacy of the citizens. As a representation of the collective citizens, different advocacy groups can exercise pressures to the agencies as well as conduct privacy awareness programs which ultimately would secure the privacy indirectly. "*It is not always possible to raise my [own] voice against privacy because I do not have a platform … the [representatives of the] civic society should take a leadership role and work as a watch-dog [protesting a privacy violation]*". Moreover, they suggested that, the government (agencies) must take initiative to improve the level of public knowledge and understanding about potential privacy issues related to RFID. Alternatively, such type of publicity and public-awareness help the success of this technology as it removes ambiguity among the citizen. Moreover, opinion leaders can be engaged for public dialogue in the mass media; technology promoting agencies too can contribute in the process. Therefore, the roles of the communication channels are twofold: exercising pressure to the agencies to ensure privacy; and disseminating RFID-knowledge among the citizens. The final hypothesis hence is developed as follows:

Hypothesis 6 Communications channels will increase users' confidence regarding privacy issues.

Figure 1 presents the antecedents of perceived privacy in public use of RFID technology, with their relations.

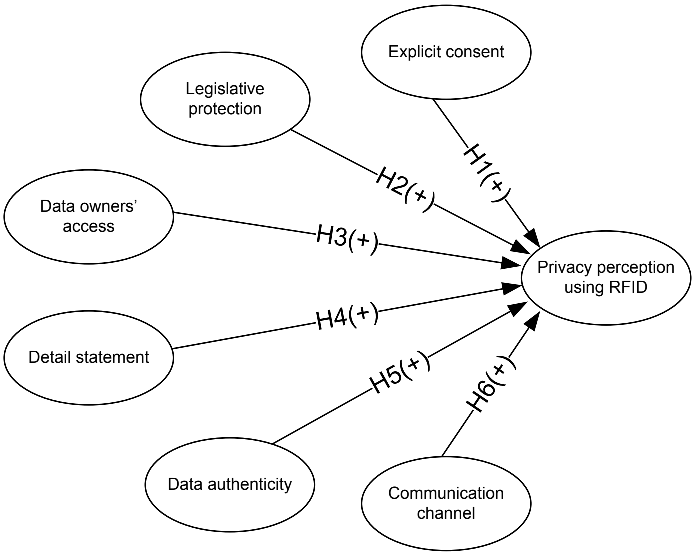

Figure 1 The proposed model for privacy perceptions in public use of RFID technology

5. The Empirical Study

5.1 Data collection

A questionnaire has been developed from the current literature and the results from the field study, in English; however, a translated version has been used for the Bangladesh sample. The translation was performed by a professional translator accredited by NAATI. The constructs were operationalized as reflective. For the survey, questionnaires were distributed among the commuters in Perth (Australia) and Dhaka (Bangladesh). In order to find responses from various segments, the survey was conducted in three consecutive week-days and in weekend. Moreover, three different routes in each sample have been covered. Overall, 156 responses from Perth and 185 from Dhaka-sample were usable.

5.2 Data Analyses and Results

The current study applied component-based structural equation modelling (SEM) using PLS, considering its suitability over covariance-based SEM. While assessing the measurement properties, first, the item loadings have been examined. The research model consisted of 28 manifest variables; considering 0.6 as the minimum cut-off level (Igbaria, Guimaraes, & Davis, 1995), two items were discarded from Australian sample, which is three in Bangladeshi sample. Then, the composite reliability (CR) and average variance extracted (AVE) were checked to assess the internal consistency of the model. Referring to Table 1, all constructs met the acceptable criterion for composite reliability (0.7 or more) and AVE (0.5 or more) (Henseler, Ringle, & Sinkovics, 2009).

Table 1 Item loadings, composite reliability and AVE of the constructs

Construct	*Item*	*Loading (Australia)*	*Loading (Bangladesh)*
Explicit consent	The forms I form clearly state that:		
	. Data will not be used for other purposes than mentioned	0.727	0.828
	. Relevant agencies may share the data	0.776	0.658
	. Data can be shared before I refuse (opt-out)	0.612	0.691
	Data not shared till I permit (opt-in)	0.608	0.644
Detail statement	While the agencies collect persona data, they clearly declare:		
	. The purpose	0.488[d]	0.745
	. The method	0.643	0.818
	. Where data will be used	0.668	0.775
	. How data will be secured	0.726	0.724
	. Who will access	0.908	0.719
Legislative protection	The legislations protecting personal privacy are:		
	. serious against unauthorized access	0.789	0.728
	. sufficient to combat with cotemporary technologies	0.802	0.840
	. strong enough to secure my personal data	0.705	0.661
	. practiced regularly	0.614	0.484 [d]
Data owners' access	I am given access to check my data	0.829	0.707
	I can modify my personal data when required	0.855	0.843
	Data modification is hassle-free	0.858	0.689
	I contribute to the quality of my personal data	0.821	0.450 [d]
Data authenticity	I perceive that my personal data are secured with proper technologies	0.804	0.355 [d]
	The database that contain my personal data is secured	0.832	0.775
	The people who handle my personal are trustworthy	0.858	0.880
	My personal data are handled by trained people	0.719	0.625
Communication channel	Newspaper/magazines publish issues on RFID-privacy	0.429[d]	0.623
	Television/radio broadcasts issues on RFID-privacy	0.647	0.886
	Community leaders demonstrate on RFID-privacy	0.819	0.884
	Privacy advocates are serious on RFID issues	0.861	0.775
Perceived privacy	Privacy is a serious concern to me	0.875	0.897
	It is important to me to control the amount of access that government agencies have on my personal data	0.841	0.929
	I am not willing to share my personal information with companies who are not associated	0.735	0.911

d – discarded item

In order to check the discriminant validity at construct level, the inter-correlation of the latent variables have been checked; the square root of AVEs exceeds the inter-correlations of the constructs with the other constructs in the model (see Table 2a, 2b). Moreover, the cross-loading matrix (for each sample) was developed, but is not provided to save space; no item loads higher value on other constructs than on the construct it represents – confirming the discriminant validity at item level (Wynne W Chin, 2010; Igbaria et al., 1995).

Table 2a Inter-correlations of the constructs of Australian sample

Construct	*CR*	*AVE*	*(1)*	*(2)*	*(3)*	*(4)*	*(5)*	*(6)*	*(7)*
Privacy (1)	0.895	0.740	**0.860**						
Explicit consent (2)	0.742	0.428	0.241	**0.654**					
Detail statement (3)	0.868	0.569	0.333	0.487	**0.754**				
Legislative protection (4)	0.795	0.501	0.273	0.488	0.620	**0.707**			
Data owners' access (5)	0.855	0.597	0.767	0.135	0.272	0.280	**0.773**		
Data authenticity (6)	0.837	0.564	0.648	0.133	0.268	0.245	0.666	**0.751**	
Communication channel (7)	0.828	0.552	0.662	0.284	0.449	0.405	0.699	0.668	**0.743**

*Bold diagonal values are square root of AVE of relevant construct

Table 2b Inter-correlations of the constructs of Bangladeshi sample

Construct	*CR*	*AVE*	*(1)*	*(2)*	*(3)*	*(4)*	*(5)*	*(6)*	*(7)*
Privacy (1)	0.937	0.832	**0.912**						
Explicit consent (2)	0.800	0.503	0.644	**0.709**					
Detail statement (3)	0.870	0.573	0.695	0.612	**0.757**				
Legislative protection (4)	0.814	0.597	0.698	0.603	0.728	**0.772**			
Data owners' access (5)	0.815	0.597	0.727	0.532	0.723	0.693	**0.773**		
Data authenticity (6)	0.819	0.606	0.643	0.465	0.627	0.625	0.607	**0.778**	
Communication channel (7)	0.874	0.639	0.608	0.615	0.713	0.655	0.713	0.637	**0.799**

*Bold diagonal values are square root of AVE of relevant construct

For assessing the structural model, bootstrap method was applied in PLS. The model accounted for 65.1% and 80.8% of the variance in *perceived privacy* with the Australian and Bangladeshi sample, respectively; both values are 'substantial' and acceptable for the current study (Henseler et al., 2009). The structural properties of the causal paths including standardized path coefficients, standard error (SE), and *t*-values for each sample in the hypothesized model are presented in Table 3. The results with Australian sample summarize that, *perceived privacy* is positively associated with *data owners' access*, *data authenticity*, and *explicit consent*; while, *communication channel* will have a negative role. Similarly, the Bangladeshi respondents find that, *perceived privacy* is positively associated with *explicit consent*, *detail statement*, and *communication channel*. In both samples, the other hypotheses are partially supported (hypothesized direction of path-coefficient but with insignificant *t*-value).

Our analysis is extended to multi-group analysis: to test the separate effects of the constructs on each model; which is done by comparing the pairs of path coefficients for identical models but based on different samples, with data collected in two different countries (Henseler & Fassott, 2010). In this analysis, the Smith-Satterwait test was employed because the samples are not distributed normally and the variances of these groups are assumed different (W.W. Chin, 2000; Moores & Chang, 2006). According to this procedure, a *t*-test is calculated by the following equation:

$$t = \frac{\left|path_{sample\ 1} - path_{sample\ 2}\right|}{\sqrt{(SE_{sample1}^2 + SE_{sample2}^2)}}$$

The '$\text{path}_{\text{sample}}$' refers to the value of the path coefficient according to the subgroup, whereas SE refers to the standard error of the subgroup. Information for both was gathered from the bootstrapping sample procedures. The results are inserted in the last column of Table 3. It is found that *detail statement*, *data owners' access*, and *communication channel* have different role in different countries.

Table 3 Test of the hypotheses and the multi-group (MG) analysis

Construct to perceived privacy	Australian sample (n=156)			Australian sample (n=185)			Multi-group result
	β value	SE	*t* value	*β* value	SE	*t* value	
Explicit consent	0.127	0.065	1.967*	0.291	0.076	3.850***	1.65
Detail statement	0.009	0.068	0.132	0.295	0.083	3.540***	2.65*
Legislative protection	0.021	0.071	0.303	0.006	0.067	0.094	0.15
Data owners' access	0.687	0.118	5.828***	0.097	0.091	1.063	3.95***
Data authenticity	0.255	0.087	2.941**	0.099	0.108	0.916	1.13
Communication channel	-0.181	0.097	2.130*	0.428	0.135	3.177**	3.67***

*Significance level *p<0.05, **p<0.005, ***p<0.001*

6. Discussion and Implications

Both Australian and Bangladeshi samples admit that, *explicit consent* would enhance users' confidence regarding privacy issues; yet, the impact is larger in the latter sample. The Australians already have been practicing such consents and 'getting disappointed' seeing the non-significant influence of such provision in practice; however, Bangladeshis are still optimistic though are "far away" from practicing such consents. The Australian Senate Committee's Report on Information Technology of November 2000 (popularly known as *Cookie Monster? Privacy in the information society)* recommends for implicit consent and opt-out method of personal data collection. However, the current study recommends for a modification of the more-than-a-decade year old report to explicit consent using opt-in approach. Similarly, the other sample admits that, peoples' privacy perception toward RFID technology will be positive if the agencies provide a clear and complete consent about the data collection. The multi-group analysis reveals that, there is no statistical difference between the two groups and both admit the role of *explicit consent*.

The Bangladeshi sample support that there is a significant and positive relationship between *detail statement* of data collection process and perceived privacy of the citizens using RFID technology. However, the Australian sample rejects such relationship which is even strongly supported by the multi-group analysis. This finding emphasizes that, while collecting personal data, a detail statement regarding the use and discloser of data should be provided. All the items (except one in Australian sample) of detail privacy received acceptable item loading which supplies a guideline to the government agencies; while providing the statement. To be more specific, it should clearly mention about the purpose of data collection, the method of data collection, where the data will be used, how they will be secured, and who would access on it. As a guideline, in order to avoid any confusion and misuse the statement, “the privacy statement be on the same page as the form or prominently linked to it” (McDonagh, 2002, p. 335).

Both samples reject that *legislative protection* may enhance peoples’ confidence regarding information privacy; moreover, the multi-group analysis established that the respondents from both samples perceive in a same direction. However, if there is any, the influence would be positive in both countries, while is perceived as more influential in Australian sample, which is supported by prior studies (e.g. McDonagh, 2002). Bangladeshi people express their frustration that government is the supreme authority that could ensure their privacy, but the government itself regularly abuse the citizens’ data. Therefore, they argue that, when the government itself violates the law, no legislation would protect them from privacy abuse. Similarly, although from different aspect, the Australian citizens believe that mere government legislations cannot protect their privacy, a holistic approach that interconnects the competence of different agencies should be in practice; but, first, the government need to build trust among the citizens (Cullen & Reilly, 2008).

Regarding *data owners’ access*, the Australian respondents highly believe that, later on, the data owners’ should get the unconditional access to manipulate the data (e.g. add, delete, modify, and retrieve); however, the Bangladeshi sample partially support such notion – the difference in opinion is further supported by the multi-group analysis. Actually, citizens from developed countries want to check their private data often, and feel more empowered when they enjoy the access to their personal data – therefore, the citizen should get themselves be concerned on privacy data (Thiesse, 2007). In practice, it is already found that many countries (including Argentina, Canada) ensure that citizens can access information collected about them, can challenge the accuracy of the information and can request to correct their personal information, held by federal government organizations (Argentine-Government, 2008; Canadian-Government, 2009). However, supported by the findings in the qualitative part of this current study, the Bangladeshi respondents are sceptical about their access and control on the database; they rather would for the government agencies to come to them and manipulate the data when the government requires.

Regarding *data authenticity* to secure information privacy, the samples differ; the Australian sample accepts but the Bangladeshi sample rejects such relationship. To enhance citizens’ privacy, data should be secured by implementing contemporary techniques and technologies; furthermore, the relevant agencies should monitor the privacy parameters alongside. It should also be interpreted from Bangladesh sample that, technical and technological solutions are complimentary to the non-technical issues; in fact, most of the reported privacy abuses point the finger not to the technological solutions, but to the people who actually manage that (Davies, 1996).

Finally, since its deployment in different industries, RFID has caught a huge attention to the media people and the privacy advocacy groups – which is generally negative (Thiesse, 2007). A lot of rumours and speculations than facts actually dominate the Internet (e.g. blogs) and the physical world that may develop negative perceptions especially on the borderline people, while sometimes they educate the users as well. As seen in the Australian sample, *communication channel* deters citizens forming positive perception on privacy. As the technique of producing antibiotic from the source itself, the *communication channels* could be used to disseminate the positive potentials of RFID technology, while offcourse putting pressure to the respective agencies not to compromise the privacy of the users. Moreover, open discussion with users, agency officials, and the technologists may play an important role (Thiesse, 2007). Even, the intellectuals may initiate broad and open debate and develop the course of actions where technology will be used for human benefits, not to make people as "the servants of technology" (Can 2005). Therefore, opinion leaders and privacy advocacy groups should examine the potential privacy-risks and propose the solution, refusing the technology in national use cannot be a solution, in most cases. As the Bangladesh sample suggests, *communication channels* can enhance the awareness regarding privacy and exercising pressure on government to enhance privacy probations and against privacy breaches. Similarly, government can use various communication channels to enhance public awareness on privacy issues.

7. Conclusions

7.1 Limitations and Future Research Directions

Few limitations of the current study are worthwhile to mention so that they can be addressed in future. First, the nature of this research was exploratory: developing and validating a theory: what are the antecedents of perceived privacy. In doing so, we explored the antecedents and examined their effect on perceived privacy. Future studies could adapt the behavioural adoption-diffusion theories/models integrating the relevant established constructs (*perceived trust*, for instance) along with *perceived privacy* and the indirect effect of the six antecedents, explored in the current study. Moreover, the interrelation among the constructs (e.g. communication channel on legislative protection) can be examined. The second limitation is actually associated with using the multi-group analysis. This study used two separate samples from two different countries using same questionnaire; the questionnaire was translated from English to Bengali - the translation may have led to a change in meaning for some question-statements, which eventually may "artificially inflate" the differences in two samples (Kock, 2013). Third, this study adopted cross-sectional survey collecting responses from population at a single given time; but, privacy perceptions may reshaped after using for a while, in different applications. Hence future longitudinal data would confirm the variance, if there is any. Finally, the field studies and the surveys were conducted in two cities of the two countries. Therefore, the samples not necessarily represent the population properly. Future study could investigate the model in representative cities and address the differences, if any.

7.2 Theoretical contribution

Human rights are both consequence as well as prerequisite of a democratic society. The consequence of perceived privacy on adoption intention of RFID technology is comparatively well researched, especially in the context of retail customers (e.g. Hossain & Prybutok, 2008); however, most of them failed to explore its antecedents. Also, the behavioural solutions protecting privacy is comparatively less-studied; Eckfeldt (2005) argued that, the key to a successful acceptance of RFID technology is “how it considers the equation from consumers’ point of view”. Hence, a general ‘equation’ is – people will accept RFID technology by lowering the risk of losing their personal data, but the question remains unsolved how the privacy risks can be reduced. More glaringly, privacy study in public use of RFID is even least studied whereas RFID is increasingly adopted in public applications. The current study is a single initiative that explores the dimensions for securing *privacy* in the context of RFID-use in public applications and validates them with survey data, obtained from two countries. Therefore, the current study contributes significant knowledge in information privacy domain, especially when citizens use technologies in government-introduced-and-managed applications.

From an extensive filed study conducted in Australia and Bangladesh, the antecedents of perceived privacy have been explored, contextualized with existing literature, and propose a research model; then, the model has been validated with data obtained from two surveys conducted in these two countries. The empirical results established that explicit consent, data owners’ access, and data authenticity have positive impact toward privacy perceptions of Australian people, while communication channel has negative impact. The same model has been tested in Bangladesh and found that, explicit consent, detail statement, and communication channel have positive effect on privacy perceptions. This study also performed a multi-group analysis and revealed that the two samples differ in perception regarding detail statement, data owners’ access, and communication channel.

Acknowledgement: The authors would like to thank the Editor and the anonymous reviewers for their constructive comments and suggestions for improvement of this paper

REFERENCES

Akhtar, Muhammada Iyahiya. (2001). *Electoral corruption in Bangladesh*: Ashgate Pub Limited.

Argentine-Government. (2008). *Argentina: changes to the data protection act*.

Bailey, Stuart GM, & Caidi, Nadia. (2005). How much is too little? Privacy and smart cards in Hong Kong and Ontario. *Journal of Information Science, 31*(5), 354-364.

Baird, J. (2012). Passport Canada's fee-for-service proposal to parliament. Retrieved 04 March, 2013, from http://www.pptc.gc.ca/publications/consultations/proposition-eng.pdf

Brown, Irwin, & Russell, John. (2007). Radio frequency identification technology: An exploratory study on adoption in the South African retail sector. *International Journal of Information Management, 27*(4), 250-265.

Canadian-Government. (2009). Privacy Legislation in Canada. Retrieved 04 March, 2013, from http://www.priv.gc.ca/fsfi/02_05_d_15_e.cfm#contenttop

Capgemini. (2005). RFID and Consumers. What European Consumers Think About Radio Frequency Identification and the Implications for Business. Retrieved October 9, 2009, from www.capgemini.com/news/2005/Capgemini_European_RFID_report.pdf

Cas, Johann. (2005). Privacy in pervasive computing environments-a contradiction in terms? *Technology and Society Magazine, IEEE, 24*(1), 24-33.

CASPIAN. (2003). Position Statement on the Use of RFID on Consumer Products. Retrieved 28 October, 2013

Chin, W.W. (2000). Frequently Asked Questions - Partial Least Squares & PLS-Graph from http://plsgraph.com/

Chin, Wynne W. (2010). How to write up and report PLS analyses. In V. E. Vinzi, W. W. Chin, J. Henseler & H. Wang (Eds.), *Handbook of Partial Least Squares* (pp. 655-690). Germany: Springer.

Chong, Alain Yee-Loong, & Chan, Felix TS. (2012). Understanding the Acceptance of RFID in the Healthcare Industry: Extending the TAM Model *Decision-Making for Supply Chain Integration* (pp. 105-122): Springer.

Coblentz, William K, & Warshaw, Robert S. (1956). European Convention for the Protection of Human Rights and Fundamental Freedoms. *California Law Review, 44*(1), 94-104.

Cullen, Rowena, & Reilly, Patrick. (2008). Information Privacy and Trust in Government: a citizen-based perspective from New Zealand. *Journal of Information Technology & Politics, 4*(3), 61-80.

Culnan, M.J., & Bies, R.J. (2003). Consumer privacy: balancing economic and justice considerations. *Journal of Social Issues, 59*(2), 323–342.

Davies, Simon. (1996). *Big Brother: Britain's web of surveillance and the new technological order*: Pan.

Directive, EU. (1995). 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. *Official Journal of the EC, 23*, 6.

Dwivedi, Y.K. (2008). *Consumer adoption and usage of broadband*: IGI-Global.

Dwivedi, Y.K., Kapoor, K.K., Williams, M.D., & Williams, J. (2013). RFID systems in libraries: An empirical examination of factors affecting system use and user satisfaction. *International Journal of Information Management, 33*, 367-377.

Eckfeldt, Bruce. (2005). What does RFID do for the consumer? *Communications of the ACM, 48*(9), 77-79.

Farjana. (2012). Speakers demanded privacy and data protection law in the national convention. Retrieved 28 October, 2013

Floerkemeier, Christian, Schneider, Roland, & Langheinrich, Marc. (2005). Scanning with a purpose–supporting the fair information principles in RFID protocols *Ubiquitous Computing Systems* (pp. 214-231): Springer.

Fosso Wamba, Samuel, Anand, Abhijith, & Carter, Lemuria. (2013). A literature review of RFID-enabled healthcare applications and issues. *International Journal of Information Management, 33*(5), 875-891.

Gilbert, A., & Shim, R. (2003). Wal-Mart cancels 'smart shelf' trial. Retrieved 4 March, 2013, from http://news.cnet.com/2100-1017_3-1023934.html

Günther, Oliver, & Spiekermann, Sarah. (2005). RFID and the perception of control: the consumer's view. *Communications of the ACM, 48*(9), 73-76.

Henseler, Jörg, & Fassott, Georg. (2010). Testing moderating effects in PLS path models: An illustration of available procedures *Handbook of partial least squares* (pp. 713-735): Springer.

Henseler, Jörg, Ringle, Christian, & Sinkovics, Rudolf. (2009). The use of partial least squares path modeling in international marketing. *Advances in International Marketing (AIM), 20*, 277-320.

Hong-Kong-Government. (2012). *The Hong Kong Personal Data (Privacy) Ordinance 2012*. Office of the Privacy Commissioner for Personal Data Retrieved from http://www.gld.gov.hk/egazette/pdf/20121627/es12012162718.pdf.

Hossain, M.M., & Prybutok, V.R. (2008). Consumer Acceptance of RFID Technology: An Exploratory Study. *IEEE Transactions on Engineering Management, 55*(2), 316 - 328

Igbaria, Magid, Guimaraes, Tor, & Davis, Gordon B. (1995). Testing the determinants of microcomputer usage via a structural equation model. *Journal of Management Information Systems, 11*(4), 87-114.

Jordan, R. (2010). Identity cards and the access card.Parliament of Australia. Retrieved 4 March, 2013, from http://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/Publications_Archive/archive/identitycards

Juels, Ari. (2006). RFID security and privacy: A research survey. *Selected Areas in Communications, IEEE Journal on, 24*(2), 381-394.

Juels, Ari, Molnar, David, & Wagner, David. (2005). *Security and Privacy Issues in E-passports.* Paper presented at the Security and Privacy for Emerging Areas in Communications Networks, 2005. SecureComm 2005. First International Conference on.

Karjoth, Günter, & Moskowitz, Paul A. (2005). *Disabling RFID tags with visible confirmation: clipped tags are silenced.* Paper presented at the Proceedings of the 2005 ACM workshop on Privacy in the electronic society.

Kelly, Eileen P, & Erickson, G Scott. (2005). RFID tags: commercial applications v. privacy rights. *Industrial Management + Data Systems, 105*(5/6), 703-713.

Kock, Ned. (2013). Advanced mediating effects tests, multi-group analyses, and measurement model assessments in PLS-based SEM (pp. 1-14). Laredo, Texas: Script Warp Systems.

Kowlessar, Geisha. (2012). e-passports by 2017. http://guardian.co.tt/news/2012-12-06/warner-e-passports-2017

Langheinrich, Marc. (2009). A survey of RFID privacy approaches. *Personal and Ubiquitous Computing, 13*(6), 413-421.

Laudon, Kenneth C, & Laudon, Jane. (2012). *Management Information Systems: Managing the Digital Firm* (12 Ed.). New Jersey: Prentice Hall.

Leimeister, Stefanie, Leimeister, Jan Marco, Knebel, Uta, & Krcmar, Helmut. (2009). A cross-national comparison of perceived strategic importance of RFID for CIOs in Germany and Italy. *International Journal of Information Management, 29*(1), 37-47.

Masnick, M. (2003). Wal-Mart Cancels RFID Smart-shelf Trial. Retrieved 4 March, 2013, from http://www.techdirt.com/articles/20030709/1138246.shtml

McDonagh, Maeve. (2002). E-government in Australia: the challenge to privacy of personal information. *International Journal of Law & Information Technology, 10*(3), 327-343.

Moores, Trevor T., & Chang, Jerry Cha-Jan. (2006). Ethical Decision Making in Software Piracy: Initial Development and Test of a Four-Component Model. *MIS Quarterly, 30*(1), 167-180.

Murray, Charles J. (2003). Privacy concerns mount over retail use of RFID technology. *Electronic Engineering Times, 1298*, 4-5.

Ohkubo, Miyako, Suzuki, Koutarou, & Kinoshita, Shingo. (2005). RFID privacy issues and technical challenges. *Communications of the ACM, 48*(9), 66-71.

Peslak, Alan R. (2005). An Ethical Exploration of Privacy and Radio Frequency Identification. *Journal of Business Ethics, 59*, 327-345. doi: 10.1007/s10551-005-2928-8

RFID-Journal. (2005). What is RFID? Retrieved 01/08, 2011, from http://www.rfidjournal.com/article/view/1339/1/129

Rognehaugh, Richard. (1999). *The health information technology dictionary*: Aspen Publishers.

Sareen, B. (2005). Asia: billions awaken to RFID. In S. Garfinkel & B. Rosenberg (Eds.), *RFID* (pp. 451–466). Upper Saddle River, NJ: Addison-Wesley.

Saunders, L. (2008). ID Cards for Australian?, *ABC News*. Retrieved from http://www.abc.net.au/unleashed/31898.html

Sutanto, Juliana, Palme, Elia, Tan, Chuan-Hoo, & Phang, Chee Wei. (2013). Addressing the personalization-privacy paradox: an empirical assessment from a field experiment on SmartPhone users. *MIS Quarterly, 37*(4).

Thiesse, Frédéric. (2007). RFID, privacy and the perception of risk: a strategic framework. *The Journal of Strategic Information Systems, 16*(2), 214-232.

Thomas, M. (2004). Is Malaysia's Mykad -the One Card to Rule Them All-The Urgent Need to Develop a Proper Legal Framework for the Protection of Personal Information in Malaysia. *Melbourne University Law Review*.

Thornley, Clare, Ferguson, Stuart, Weckert, John, & Gibb, Forbes. (2011). Do RFIDs (radio frequency identifier devices) provide new ethical dilemmas for librarians and information professionals? *International Journal of Information Management, 31*(6), 546-555.