EXPLORING THE PERCEIVED MEASURES OF PRIVACY: RFID IN PUBLIC APPLICATIONS

Mohammad Alamgir Hossain
School of Business, North South University
Dhaka, BANGLADESH
Email: mahripon@yahoo.com

ABSTRACT

The purpose of this study is to explore the measures that may protect privacy of the users - in the context of RFID use in public applications. More specifically, this study investigates what the users perceive to have securing their privacy, particularly for the RFID applications in public uses. Qualitative research approach has been utilised for this study. The author conducted two focus-group discussion sessions and eight in-depth interviews in two countries: one from Australasia region (Australia) and the other from Asia (Bangladesh), assuming that the status, and the perceptions and tolerance of the citizens on privacy issues are different in the stated regions. The explored factors have been analysed from privacy perspectives. The findings show that, in developed and developing countries, the basic perceptions of the users on privacy protection are complimentary; however, privacy is a more serious concern in Australia than in Bangladesh. Data analysis proposed some attributes that may improve users' privacy perceptions when RFID is used in public applications. This study is the single initiative that focuses on privacy of RFID users from national-use context. As practical implication, the proposed attributes can be exercised by the deploying agencies that implement RFID technology for citizens' use.

Keywords: RFID; national ID; Smart-ID; privacy; e-passport; qualitative study

INTRODUCTION

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). In industrial and supply chain applications, RFID technology can trace a product through its entire lifecycle - from the production line to all the way to the recycling centre (Lin 2009). Many countries have developed and implemented RFID-based human identification system that uses the data obtained from this system for various national administrative purposes and/or to provide specific services to the citizens. National Identity (ID) cards and electronic passports (e-passport) are the main applications that governments are more interested-in because in recent times governments are more serious to combat potential terrorism activities and crimes.

In national-level public applications of RFID, the captured data about the citizens is accessed, handled and shared by many departments or authorities. For instance, the proposed (but failed) national identification system 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 special attention from the deploying authorities to keep the data confidential and inaccessible to any unauthorized use (Kelly & Erickson 2005; Vaudenay 2006). 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. Citizens' privacy can be abused if the data is accessible to any unauthorized or unlawful person(s)

and/or if the data is supplied to any unauthorized third party. In fact, 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 perceptions protecting privacy with highest priority. Privacy International specifically suggested that China and Malaysia need to be serious about privacy; both countries are using RFID in public applications extensively while their privacy ranking is worst in the world (Privacy International 2006). Although most RFID researchers are obsessed to develop techniques for privacy protection, the actual problem (and hence the potential solution) lies somewhere else (Hossain & Prybutok 2008). It is generally assumed that in United Kingdom "at any one time, one percent of staff will be willing to sell or trade confidential information for personal gain." (Davies 1996). Therefore, not surprisingly, there have been instances of forgery and counterfeiting of identity cards, not due to a lack of security features but due to the assistance of corrupted public-officials holding positions of trust in government (Thomas 2004). Such privacy abuse could harm more especially after the implementation of anti-terrorism laws in several countries. Hence, "effective action is needed" so that citizens "can trust that the various applications of RFID are privacy-friendly" (Langheinrich 2009). The current study explores the perceptions of the actual users which may protect and/or enhance their privacy stipulation in national applications. This study, therefore, tries to contribute to fill up this research gap by exploring the privacy catalysts of RFID use in national applications from a behavioural study.

In order to get a comparative picture, this study explores the perceptions of the users from a developed country (Australia) and a developing country (Bangladesh). In general, people in Australia are more concerned and serious about their privacy. 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 the occasions, the main concern was the 'privacy'. On the contrary, most of the Asian countries including Bangladesh, where people are believed to be more resilient on privacy, have been using national identity card for generations. This research will explore the factors that the users in these two countries (Australia and Bangladesh) perceive as important on privacy issue - particularly when they are tagged with RFID technology in the forms of public applications.

BACKGROUND

RFID in Brief

RFID is one type of automatic identification technology that uses radio wave as the way of communication (Angeles 2005). An RFID system consists of tags (transponders), readers (transceiver /interrogators) and a network system (middleware) (Finkenzeller, 1999; Wu *et al.* 2006). The tags store data. The readers scan and communicate with tags via electromagnetic wave and transmit the information on the tags to a database or data processing network through the middleware (Wu *et al.* 2006). The middleware manages the data collected from the tags, processes the data, and provides the data in real-time software systems (e.g. ERP systems) or to the Internet (Finkenzeller 2006; Wu *et al.* 2006). RFID tags come in different types according to their functionality: active or passive. Active tags have an active radio frequency (RF) transmitter and a built-in battery to power the logic chip and to communicate with readers. On the other hand, passive tags do not have any in-built power source; therefore, they need to get power from readers in order to run the digital logic on the chip and to issue a response to the reader (Plos *et al.* 2012). In this study, we focus only on passive tags due to their substantial usage in public applications and hence possess highest impact on users' information privacy.

RFID in Public Applications

An RFID card enables the system to automatically identify the bearer of the card by the means of RF. It is worthwhile to note that 'automatically' means the card does not need to be inserted or swiped but is read by an RFID system only when the card comes in a readable distance of a reader. It is not the case that the reader can read the card from nowhere; actually the operating frequency is kept low to restrict reading of the cards from far away. Most of the public applications of RFID technology use the *proximity cards* that would not be read if the tag and reader are far than 10 centimetre.

National identity card (hereinafter, SmartID[4]) is the main application of RFID technology among public. Malaysia is the first country to introduce RFID in its national identity card (MyKad) in 2001 (Tedjasaputra 2006; Thomas 2004). Several other regions including Hong Kong, Estonia, Finland, Belgium, Portugal, Spain and recently China and Albania issued Smart-ID to its citizen (ABI Research 2008; Wikipedia 2009).

The next major application of RFID in national use is the electronic passport (e-passport); RFID chip is integrated in a passport which stores data such as name, date of birth and address, as well as biometric data like facial recognition (image), fingerprint recognition and iris recognition of the bearer (Juels *et al.* 2005). Many countries have already implemented and mandated RFID-based electronic passports while many other countries are in the process. For example, since January 1, 2011 no Nigerian without an e-passport is allowed to travel into or out of Nigeria (All Africa 2010); in 2004, Canada mandated its passport issuing authority (Passport Canada) to adopt e-passport; Trinidad and Tobago motivates its citizens to have their e-passport by 2017 so that they will "be allowed to enter a foreign country … with the just swipe of a card" (Kowlessar 2012).

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 (ICAO 2009). However, the deadline has been extended to 2017 (Kowlessar 2012). Most of the countries hence already started their projects for the implementation of e-passport facilities. Till March 2012, "approximately 95 countries issued e-passports, including all ... G8 nations" (Baird 2012, p8). Similarly, as a regional pressure, European Union (EU) is on its way to implement a globally-unique cross identification process by the means of electronic identification system with the intention of sharing the IDs with allied countries for the purposes like Interpol investigations or visa-free-entry (e-Finland 2004).

Privacy Review and RFID Technology

'Privacy' is considered as a fundamental requirement to any modern democracy. A survey conducted by Capgemini (2005) revealed that *privacy* is perceived as the top concern by the RFID users. RFID (information) privacy issues is well explored in literature; however, the researchers are concerned and concentrate mainly on the technical and technological issues of item-level tagging and privacy issues

[4] We should not be confused with RFID and Smart Card. Though both technologies use Radio Frequency and contactless features, there are technological and operation differences between RFID and Smart card. In general, the read range of Smart Card is up to10 cm which is from 10 cm to 10 m for RFID cards. In this paper, Smart-ID is defined as the identification by means of RFID technology. For detail, readers are encouraged to read papers including http://www.frost.com/sublib/display-market-insight-top.do?id=83467478

of the customers in retail stores (e.g., Chong & Chan 2012; Juels 2006; Kelly & Erickson 2005; Peslak 2005). There is scant behavioural literature on the privacy issues of RFID in the context of national ID cards, commuting cards, etc. The nature of captured data, data use, and data exposure through an RFID system in a retail chain is very different from that in a public use; in fact, the latter case is more serious as it is vulnerable to civil rights violations (Hossain & Prybutok 2008; Peslak 2005). Moreover, customers may reject shopping from an RFID-enabled shop but may not refuse RFID on public use because of government law. For instance, Wal-Mart "cancelled" its RFID-based 'smart shelf' trial (Gilbert & Shim 2003) "while there have been some complaints about the privacy implications" (Masnick 2003), and many customers showed reluctance to shop. A number of privacy controversy in retail sector have been reported by Thiesse (2007). On the contrary, it is not reported yet if a citizen refuses RFID-enabled e-passport.

Privacy is a 'natural right' or 'right to be left alone'. The treaty of the European Union states that everyone's privacy right "shall be no interference by a public authority with the excercise of this right except such as is in accordance with the law and 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''(European Communities 2004). Almost similar provisions are made in the U.S. and other countries (US Congress1995). Therefore, collecting and using users' data through RFID-use in State applications is lawfully and ethically justified. However, this provision cannot be applied to retailers to disseminate customers' personal data. Hence, consumer advocacy groups are currently lobbying for privacy legislation regarding use of RFID (Whiting 2003). However, they do not object the government use of RFID for national interest (CASPIAN 2003-04), but urge and demand that under no circumstance users' personal and sensitive information should be misused. In general, *personal data* means any data (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 the Smart-IDs is personal and sensitive. Therefore, even for national interest, citizens' information has to be authentically accessed by the right personnel and lawfully be used for national interest. On the contrary, RFID in a retail chain does not keep too personal data; it finds pattern on customer's taste, purchase and so on (Cazier 2008). Therefore, RFID and citizens' privacy is more serious and requires attention, which is yet well addressed in the literature compared to that of the retail sector. For a detail review on privacy literature, see Bélanger & Crossler (2011) and Pavlou (2011); a brief is presented in Table 1.

Reference	Area	Brief findings
Sutanto *et al.* (2013)	Smart-Phone users	Provision and then personalization of privacy features are (perceived as) effective securing users' privacy
Bélanger & Crossler (2011)	Review on information privacy	Identified 23 privacy concern including unauthorized secondary access and use, risk, vulnerability
Pavlou (2011)	Review on information privacy	Pointed on the privacy paradox in literature: "an individual's concerns about information privacy do not necessarily map with the individual's intentions to share personal information"
Garfinkel *et al.* (2005)	RFID-related privacy concerns	Different privacy threat to persons: action threat, association threat, location threat, preference threat, transaction threat, breadcrumb threat
Smith *et al.* (1996)	Information privacy	Privacy concern in terms of: collection of personal information, improper/unauthorized access, unauthorized secondary use (by the organization itself that collects it, and by the other organizations that collect information from the collector organization), combining data into larger database (mosaic effect), and errors in data

Table 1 A brief examination on existing privacy studies and major findings

Irrespective of developing or developed countries there have always been some debates and lack of trust in using a strong technology like RFID which has the capability of tracking a person in real-time. Generally, privacy is a big concern especially in developed countries whereas in developing countries it is bit flexible for government-use of citizens' information. The constitutional bodies (e.g. election commission) in many developing countries (including Bangladesh), unlike the developed countries (like Australia), are not beyond the control of the government. Hence, a corrupted political government may use citizens' data for their own benefits such as political harassments to opposition parties or to manipulate election result. Moreover, discrimination on the basis of religion, past criminal record or medical history is also very prominent in Smart-ID privacy abuse cases (Thomas 2004). Furthermore, a citizen/consumer with lower personal tolerance places higher importance and sacrifices less on personal privacy (Ohkubo *et al.* 2005). Especially in the developed countries, many of the RFID projects had been cancelled because of the strong protests from the consumer advocacy groups. Along with the Wal-Mart example given earlier, Metro AG, the giant retailer in Europe "discontinued" its trial with RFID-tagged 'customer pay-back card' (Metro AG 2004). Still we see lots of potential privacy abuse cases from developed countries; for example, the State of Illinois receives around $10 million from record selling (Kurtz 1998) – the question is: do they include citizens' personal information? The answer is crucial and remains unanswered.

RESEARCH DESIGN

For this study, the qualitative method is considered as most appropriate because of the exploratory nature of the research. Scholars argue that, understanding a phenomenon from the point of the participants is difficult to achieve when textual data are quantified (Kaplan & Maxwell 1994). Therefore, a 'pseudo case study' that involved a qualitative study of a small number of participants would meet the objectives of this study. As such, field study approach has been adopted as the research method (Patton 1999; Zikmund 2000). Moreover, qualitative methods permit the evaluator to study selected issues in depth and in detail. In order to ensure the positivist stand of this research the field-study was performed without being constrained by predetermined outcomes rather relying on openness,

and detail of qualitative inquiry (Patton 1999). Correspondingly, Eisenhardt (1989) argued that qualitative study is "particularly well suited to new research areas or research areas in which existing theory seems insufficient" (p. 548-549). RFID is considered as the world's "oldest new technology" (Poirier & McCollum 2006, p3); not many studies came up with the exploration of (behaviorial) privacy measures, except a handful research from the technological perspective. Therefore, this study used multiple case based field-study approach which is considered as an appropriate research design when the purpose of the research is descriptive, theory building, and practice-based, and where the profound thoughts and experiences of the subjects are important (Benbasat *et al.* 1987).

Sampling and Data Collection

This study obtained qualitative data from two focus group discussion (FGD) sessions and eight in-depth interviews conducted with RFID users in Perth (Western Australia) and Dhaka (Bangladesh).FGD in Perth and Dhaka involved six snd seven discussants respectively. Participants were ranged in the age between 18 to 61 years and had almost equal participation from both the genders. Each session was conducted by one moderator, which lasted about 70 minutes while the average interview time was around half-an-hour. In addition, eight direct interviews (four in Perth and four in Dhaka) were conducted to explore users' insights on this current research agenda. Regarding the number of cases to investigate, opinion varies among the researchers. Some researchers suggest an open-ended number of cases while others recommend a restricted range while the most appropriate range falls between four and eight (Eisenhardt 1989). However, considering the importance of the issue, this study approached to the individuals until reaching the saturation. In both cases, participants were recruited using convenient sampling in order to ensure productive findings. The interviewees have been using at least one or more RFID applications provided by the State. The respondents from Perth use SmartRider whereas the respondents from Dhaka use SPASS – both are the ticketing cards for public transport commuting service supplied by the Western Australian Public Transport Authority and Bangladesh Road Transport Authority, respectively.

At the beginning of each interview the focus groups were given a brief outline of the RFID technology and the research purposes. The participants were informed that they could quit the interview at any time without any prejudice. Also they were informed about the usage-policy of captured data from the discussions.

In both cases a semi-structured open-ended questionnaire has been used. The respondents were allowed to discuss on the privacy issues related to 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?

Reliability was ensured by using the same interview-protocol for each session. The moderator and the interviewer inserted the questions into the discussion/conversation and prompted when needed. With the permission of the participants, the discussions/interviews were recorded. Following Seidman's (2005, p. 64) advice, while conducting the interview the interviewer of this study did not take detail written-notes, but only short notes. These 'working notes' helped the interviewer to concentrate on participant's comments. This also helped the interviewer to note a prompt question to be asked at a later stage without interrupting the participants.

Data Analysis

To examine and analyse the qualitative data, this study employed 'content analysis technique' (Siltaoja 2006) and developed relationship among relevant concepts. Among "various ways" of content analysis (Siltaoja 2006), inductive and deductive analyses were carried out (Berg 1989). In the inductive phase; themes, sub-themes, and concepts explaining variables, factors, and, sometimes, measurement scales

have been explored. In a later stage of inductive phase, the explored factors and variables have been 'induced' into a single framework. At this stage, this study followed both 'theoretical replication' as well as 'literal replication' (Chan & Ngai, 2007). Theoretical replication was made by contrasting cases among respondents, while literal replication was obtained from their similarities.

NVivo software from QSR International has been used in this study to analyse data. As claimed by Bazeley (2007, p.2), "NVivo has been developed by researchers, with extensive researcher feedback, and is designed to support researchers in the varied ways they work with [qualitative] data." Moreover, NVivo "supports analysis of qualitative data" by managing data, managing idea, permitting data query, developing graphical models, and reporting from data (Bazeley 2007; Welsh 2002). By coding the discussions/interviews word-by-word using NVivo8, a number of 'free nodes' have been developed by naming each segment of data with a label. Each 'free node' summarized and accounted for each concept about the data. Later, 'tree nodes' were developed from the free nodes. Each tree node became a prospective construct which consists a set of relevant free nodes with similar concept.

FINDINGS

Perceived by the respondents, for the success of the RFID, an efficient and flexible privacy mechanism needs to be taken by the respective agencies. The following strategic issues were discussed by the interviewees:

Explicit consent

> "*The treatment of personal data is unlawful when the data owner has not given his or her express consent which must be given in writing, or through any other similar means, depending on the circumstances*" (Argentine Government 2008).

Respondents both from Australia and Bangladesh perceive that explicit consent from the citizen is essential for securing privacy; the clear consent must would state that the "*data would not be used in a manner other than it mean to be*" (FCD 1&2), and the data owner-should sign the consent form or check the box in online form. They unanimously agreed that once the explicit consent is obtained by an agency from a citizen, the relevant stakeholders must use the data without further consent. For example, permission for accessing the contacts of the residents of an electorate by a politician through the election commission is implicitly given by the citizens. However, the respondents differ with the degree of data-sharing among the government agencies. Bangladeshi respondents are more liberal and believe that, in order to avail a service, the extent of rights can be relaxed with explicit (or even implicit) consent; that means, every government agency may share data although data may have been obtained by one agency. However, Australian respondents are more serious: "*It is not automatic to waive the privacy for every agency*" when only one agency is granted the permission (respondent 3: Australia); data collected from one public application might be used for other public applications too, but the respondents urge that the data-owner should be informed and asked every time whether the authorities can do share. They suspect that government agencies abuse the *opt-out* model of data acquisition-and-use where the citizens' information may be distributed till they refuse – "*this is a catch*". Proving the seriousness of Australians to privacy, they demand a quick shift from *opt-out* to *opt-in* model that requires citizens' consent to share their data. The first proposition, hence, is developed as follows:

Proposition 1. Explicit consent from the government agencies will increase the privacy of the citizens; yet, citizens from developed countries perceive that opt-in model is better securing citizens' privacy whereas citizens from developing countries still are comfortable with opt-out model of privacy.

Detail privacy statement

The respondents asserted that the agencies should publish and provide a detail privacy statement while collecting personal information. Ideally, the statement should include a clear, conspicuous and detail listing of methods of collecting and using data. When asked about what the things the respondents expect to see on the consent form, at least six items came up as significant which are not exhaustive: (i) why the data will be collected, (ii) how the data will be collected, (iii) how long the data will be kept, (iv) how the data will be used, (v) how the security of the personal data is preserved, and (vi) who do have the access to the data. One of the respondents overtly mentioned about some Acts from international arena: the Acts under Federal Privacy Act 1983 in Canada ensures detail explanation on how data will be collected and how such information can be used, which is further administered and watched-over by an independent commissioner or ombudsperson, with the authority to investigate complaints (checked and clarified from Canadian Government 2009). Moreover, the statement would explain the appropriate security-standards for personal information including establish security systems, conduct security audits and risk assessment, employ 'watch-dog' authority and manage security policies properly (Floerkemeier *et al.* 2005). The respondents from Bangladesh mentioned that such detail statement is very rare and may develop ambiguity and lack of confidence on government's use of citizens' data. In the context of developed countries, detail privacy statement is provided to the citizens. However, respondents from both the countries claimed that detail privacy statements would increase the confidence of the citizens toward securing their privacy. Therefore, the proposition becomes:

Proposition 2. Detail privacy statement in government forms will increase the privacy of the citizens which is available in the developed countries but not in the developing countries.

Legislative protection

> "*A record-keeper who has possession or control of a record that contains personal information shall ensure that the record is protected, by such security safeguards as it is reasonable in the circumstances to take, against loss, against unauthorized access, use, modification or disclosure, and against other misuse*" (Australian Government 2008)

The respondents in this study re-established that every country should have legislations against unauthorized access and/or use of personal data, harvested by government agencies. For instance, *Privacy Act 1983* in Canada protects the personal information collected by government institutions. "*Under no circumstance the State should tolerate any information abuse*" collected from an RFID system (respondent 2, Australia); "*lack of legislation is one of the main reasons for privacy abuse with RFID in Malaysia*" (respondent 1: Australia[5]) . They 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 that would secure public data from any source of unrestricted public-access.

[5] After a long waiting, finally in 2007, a bill was prepared, called as the bill of Personal Data Protection, in reducing the privacy deficiency was finalized to regulate the collection, processing and use of personal data in Malaysia (Khaw 2002; Kettha 2007)

Both FGDs revealed that the overall application of privacy law is better in Australia than most of the Asian countries, which is supported by McDonagh (2002). The Australian respondents believe that legislation against privacy abuse can secure their privacy; in the worst case, they can go to the court and ask for compensation. On the contrary, the Bangladeshi respondents claimed that, there is no such legislation in Bangladesh which can protect privacy of the citizens - while the movement 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 (FCD: Bangladesh). However, most of the respondents from Bangladesh believe that, the citizens should be protected by law - regardless.

One of the respondents working in academic research recommended that Governments should behave "smartly" with handling "a smart technology" like RFID. He appreciated and recommended contemporary laws 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 (US Congress 2002). Hence, it is proposed that:

Proposition 3. Legislative protection, specific to electronic data and data obtained from electronic systems, will increase the privacy of the citizens; yet, legislation is effective and better practiced in developed countries than in developing countries.

Data-owners' accessibility

The respondents believe that, to their personal information, citizens must have control over the amount of access to the data that the government agencies possess. They believe that citizens, once they have duly evidenced their identity, should have the right to obtain data and request to change the information on their personal data-field. To support their recommendation, it is found that many countries (including Argentina and Canada) ensure that citizens can access information collected about them, can challenge the accuracy of the information and can request to edit their personal information, held by federal government organizations (Canadian Government 2009; Argentine Government 2008). The Bangladeshi respondents claimed that, unfortunately, people do not have sufficient access to their data; they cannot upgrade the information on their profile "involves unnecessary hassle – both financially as well as mentally….If you want to take the initiative to let the country know about your current status, it is simply stupidity - they [the agencies] will abuse you[r responsible behaviour] (FGD 2)". Therefore, the Bangladeshi respondents are cynical about providing their personal information to government – they rather feel comfortable with private agencies. On the contrary, the Australian respondents believe that the access on their personal data is more secure and easy to access and modify. Yet, they demand that, instead of updating data by different agencies, a replicated distributed database system would be more effective. Therefore, the fourth proposition is developed as follows:

Proposition 4. Data owners' accessibility will increase the privacy of the citizens; yet, citizens from developed countries perceive that they have more control over data than that in developing countries.

Data authenticity

To ensure privacy, it is a fundamental requirement that data should be safeguarded properly – this is more critical for a technological innovation like RFID. 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 companies 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 agencies 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, the respondents 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 obsolete techniques. Hence, the next proposition can be stated as follows:

Proposition 5. Data authenticity will increase the privacy of the citizens. Developing countries have less effective data-authenticity mechanism than in developed countries; yet, agencies need to adopt contemporary mechanisms that are effective to combat hackers.

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 would ultimately secure the privacy indirectly. "*It is not always possible to raise my [own] voice against privacy because I do not have a platform and [I] might be treated as a member of opponent party … the [representatives of the] civil society should take a leadership role and work as a watch-dog [protesting a privacy violation]*" (respondent 4: Bangladesh). Similar suggestions were proposed by the Australian discussants too. They further suggested that the government (agencies) must take initiative to improve the level of public knowledge and understanding about potential privacy issues related to RFID as, in general, there is a negative 'hype' about RFID confronting privacy. Alternatively, such type of publicity and public-awareness programs would help to the success of this technology as it removes ambiguity among the citizens. Moreover, opinion leaders can be engaged for public dialogue in the mass media. Finally, technology promoting agencies can contribute to the process. Therefore, the roles of the communication channels are twofold: exercising pressure to the agencies to ensuring privacy; and disseminating RFID-knowledge among the citizens. The final proposition, hence, is developed as follows:

Proposition 6. Communication channels may increase the privacy awareness as well as privacy status of the citizens.

Figure 1 presents the dimensions of privacy in public use of RFID technology, with the propositions developed from the field study.

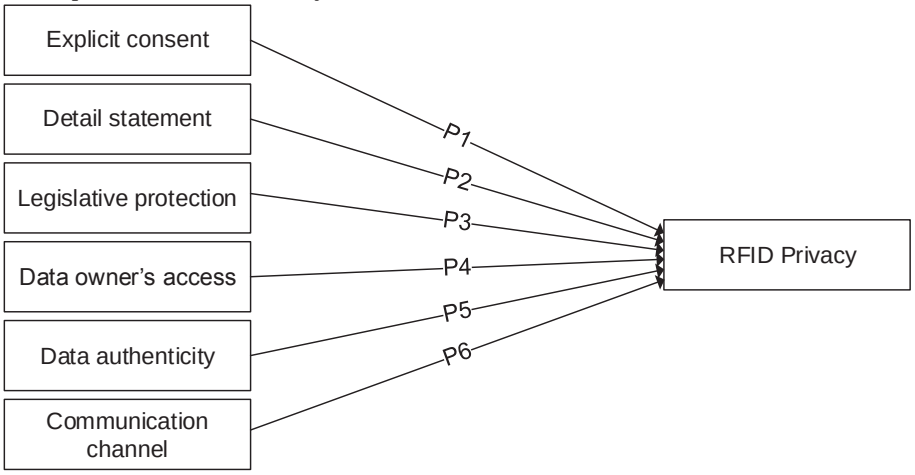

Figure 1 The proposed model for privacy dimensions in public use of RFID technology

Table 2 presents the important dimensions of perceived privacy with their respective weights. The weight is presented at percent. In total, 21 respondents were involved in this research that contributed

to 100%. It is observed that, for instance, 85% of the respondents urge for government to pass laws on citizens' data privacy and ensure its application .

Antecedents of privacy	% of respondents
Explicit consent	23
Detail privacy statement	57
Legislative protection	85
Data owners' accessibility	62
Data authenticity	28
Communication channels	38

Table 2 The variables extracted from the qualitative analysis and respective weight

DISCUSSION

Summary of Findings

One general research question drove this research – what the actual users perceive as the key strategies that can protect and enhance their privacy while they use a technology (i.e., RFID technology) - especially which can track and trace-back their movement and so on. This study conducted in-field in-depth interviews and focus group discussion sessions in a developing and in a developed country; in general, the results show that the general perceptions of the citizens on data/information privacy are not contradictory rather complimentary. The only difference exists on perception regarding the role and activities of the government regarding privacy protection in respective countries. For instance, Bangladeshi people expressed their frustration that government is the supreme authority that could ensure their privacy, but the government itself abuse the citizens' data frequently. In this case, overall, the citizens are cynical to provide their personal information to the government agencies, and simultaneously are hopeful that different pressure groups would play a significantly important role in protecting individual's data from government's abuse. On the contrary, most government agencies in Australia are autonomous and are not necessarily under the government control; therefore, data abuse by public agencies is less frequent there. In case of a violation of privacy, there is a good possibility that a citizen may receive justice (e.g. compensation) in Austalia - which is not guaranteed in Bangladesh.

Briefly, the respondents recommended some fundamental actions that need to be taken while tagging citizens with RFID technology in the form of some public applications including identity card and commuting ticketing system. The very first step to privacy protection, they recommended, is the *opt-in* approach. In contrast to the (Australian) Senate Committee's Report on Information Technology of November 2000 (popularly known as *CookieMonster? Privacy in the information society*) (McDonagh 2002) where the committee recommended for an implicit consent and *opt-out* approach of data/information collection, the current study argues for explicit and *opt-in* approach. The *opt-out* approach of informed consent permits the collection of personal information until the consumer specifically requests that the data not to be collected (Laudon & Laudon 2012). On the contrary, the *opt-in* approach prohibits a business from collecting any personal information unless the consumer specifically takes action to approve information collection (Laudon & Laudon 2012). Moreover, while collecting personal data, a detail statement regarding the use and discloser of data should be provided. To be more specific, the Privacy Commission of Australia recommends that "the privacy statement be on the same page as the form or prominently linked to it" (McDonagh 2002, p335). Later on, the data owners should get the unconditional access to control the data (e.g., change, add, delete, modify). Recent study by Sutanto *et al.* (2013) finds that the provision and then personalization of privacy

features increases Smart Phone adoption; therefore, while collecting data, citizens' should be offered with provision of privacy features (i.e. detail statement), and the right to personalizing data (i.e. access). To enhance citizen's privacy, the government can also play an important role by incepting electronic technology use-related privacy laws and also by monitoring privacy parameters. Furthermore, data should be secured by implementing contemporary techniques and technologies. Finally, opinion leaders and privacy advocacy groups can enhance privacy awareness and exercise 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.

Implications

The effect of perceived privacy on the adoption of RFID technology is well researched, especially in the context of retail customers (e.g., Hossain & Prybutok 2008). Most of these studies are mostly interested in the effect of the construct 'privacy' (mostly on adoption) but failed to explore its antecedents. Also, the behavioural solutions protecting privacy is comparatively less studied. More glaringly, privacy study in public use of RFID is even least studied whereas RFID has increasingly been adopted in public applications including national identification, passports, or commuting cards. The current study is the only initiative that explored the dimensions for securing *privacy* in the context of RFID-use in public applications. This is the first of its kind to explore the strategies to protect privacy – suggested by the actual users. Consequently, this study developed six contributing factors that enhance the privacy of the users. Hence, this study believes to have significant contribution to the existing body of knowledge in privacy and RFID studies.

In the context of privacy protection, this study demonstrated a systematic guideline for the government agencies that implement RFID technology in public use. It underscores that, in order to enhance the perceptions of the citizens on privacy, the respective agency must consider the privacy issues of the users seriously. More importantly, this study presents the components of privacy measures so that the agency can check their status and adjust their action. Moreover, it suggests that, privacy advocates should monitor the privacy status and exercise pressure on specific concern. Similarly, technology manufacturers and vendors may use different communication channels to enhance the privacy perception of the users.

Limitations and Future Research Directions

The main objective of this research was exploratory. In future, the dimensions can be validated with empirical data and may compare the differences in perceptions and their respective effects in developed and developing countries. Moreover, this study involved the respondents who use only a single RFID-application (e.g., ticketing in public commuting service). However, future research would consider simultaneous use of more applications which will provide a more detail picture. Furthermore, adapting the traditional behavioural theories and models such as Technology Acceptance Model (TAM), future study may develop an adoption-diffusion model investigating the use of RFID in public use; along with other relevant constructs, the direct effect of perceived privacy and the indirect effect of the six dimensions explored in the current study on adoption and perceived trust, for instance, may be investigated.

CONCLUSION

In many countries, government is the major driving force for RFID adoption and diffusion. Simultaneously, the government is supposed to be the largest body to secure the privacy of the RFID users. Therefore, a holistic approach to privacy management is necessary for RFID's success. From a field study, conducted in Bangladesh and Australia, this paper proposed six dimensions that might

capture the privacy perceptions of the citizens. The detail nature of the privacy concern explored from the respondents of two different countries and from various backgrounds is the main strength of this study that also provides theoretical and practical implications.

REFERENCES

ABI Research (2008) RFID moving beyond Chinese national ID program, *ABI Research*.http://www.ccidreport.com/market/article/content/3377/200803/178552.htmlaccessed 04 March 2013.

All Africa (2010) *Nigeria: e-Passport Deadline*. http://allafrica.com/stories/201004190825.html accessed 04 March 2013.

Angeles, R. (2005) RFID technologies: supply chain applications and implementation issues, *Information Systems Management* 22(1): 51-66.

Argentine Government (2008) Argentina: changes to the data protection act. *World Data Protection Report*.

Australian Government (2008) *Information Privacy Principles*. http://www.privacy.gov.au/materials/types/infosheets/view/6541#d accessed 04 March 2013.

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

Bazeley, P. (2007) *Qualitative Data Analysis with NVivo*. Sage Publications, Thousand Oaks, CA.

Bélanger, F. and Crossler, R.E. (2011) Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly* 35(4): 1017-1042.

Benbasat, I., Goldstein, D.K. and Mead, M. (1987) The case research strategy in studies of Information Systems. *MIS Quarterly* 11(3): 369-386.

Berg, B. (1989) *Qualitative research method for the social science*. Allyn and Bacon, Boston, USA.

Chan, S.C.H. and Ngai, E.W.T. (2007) A qualitative study of information technology adoption: How ten organizations adopted Web-based training. *Information Systems Journal* 17(3): 289-315.

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

Capgemini (2005) *RFID and Consumers. What European Consumers Think About Radio Frequency Identification and the Implications for Business*. www.capgemini.com/news/2005/Capgemini_European_RFID_report.pdf

Caspian (2003-04) *Position Statement on the Use of RFID on Consumer Products*. http://www.spychips.com/jointrfid_position_paper.html accessed 04 March 2013.

Cazier, J. A., Jensen, A. S. and Dave, D. S. (2008) The impact of consumer perceptions of information privacy and security risks on the adoption of residual RFID technologies. *Communications of the Association for Information Systems*, 23(14): 235-256.

Chan, S.C.H. and Ngai, E.W.T. (2007) A qualitative study of information technology adoption: how ten organizations adopted Web-based training, *Information Systems Journal* 17(3): 289-315.

Chong, A. Y-L and Chan, F. S. (2012). Understanding the acceptance of RFID in the healthcare industry: extending the TAM model, in *Decision-Making for Supply Chain Integration: Decision Engineering*, Volume 1, Springer, pp. 105-122.

Khaw, L.T. (2002) Towards a personal data protection regime in Malaysia, *Journal of Malaysian and Comparative Law* (11), http://www.commonlii.org/my/journals/JMCL/2002/11.html.

Davies, S. G. (1996) *Big Brother: Britain's Web of Surveillance and the New Technological Order*, London: Pan Books.

e-Finland (2004) Pan-European Electronic Identity Being Developed, in *Wide Cooperation. e-Government Articles*.

Eisenhardt, K.M. (1989) Building theories from case study research, *The Academy of Management Review* 14(4): 532-550.

European Communities (2004) *European convention for the protection of human rights and fundamental freedoms, Article 8*.

Farjana (2012) *Speakers demanded privacy and data protection law in the national convention*. http://www.voicebd.org/node/361 accessed 04 March 2013.

Finkenzeller, K. (1999) *RFID Handlook: Radio-Frequency Identification Fundamentals and Applications*. John Wiley & Son, Chippenham.

Floerkemeier, C., Schneider, R. and Langheinrich, M. (2005) Scanning with a purpose – supporting the fair information principles in RFID protocols, in *Ubiquitous Computing Systems*, Berlin: Springer / Heidelberg, pp. 214-231

Garfinkel, S.L., Juels, A. and Pappu, R. (2005) RFID privacy: An overview of problems and proposed solutions. *Security & Privacy, IEEE* 3: 34-43.

Gilbert, A. and Shim, R. (2003) Wal-Mart cancels 'smart shelf' trial, in *CNet News*. http://news.cnet.com/2100-1017_3-1023934.html accessed 04 March 2013.

Hong Kong Government (2012) *The Hong Kong Personal Data (Privacy) Ordinance 2012. Office of the Privacy Commissioner for Personal Data*. http://www.gld.gov.hk/egazette/pdf/20121627/es12012162718.pdf accessed 04 March 2013.

Hossain, M. and Prybutok, V. (2008) Consumer acceptance of RFID technology: an exploratory study, *IEEE Transactions on Engineering Management* 55(2): 316-328.

ICAO (2009) *International Civil Aviation Organization*. http://www.icao.int/cgi/statesDB4.pl?en accessed 04 March 2013.

Jordan, R. (2010) *Identity cards and the access card.Parliament of Australia*. http://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/Publications_Archive/archive/identitycards accessed 04 March 2013.

Juels, A. (2006) RFID security and privacy: a research survey, *IEEE Journal on Selected Areas in Communications*, 24(2):1-19.

Juels, A., Molnar, D. and Wagner, D. (2005) Security and privacy issues in e-passports, *First International Conference on Security and Privacy for Emerging Areas in Communications Networks*, pp. 74-88: http://www.library.ca.gov/crb/rfidap/docs/Juelsetall-SecurityandPrivacyofE-Passports.pdf

Kaplan, B. and J.A. Maxwell. (1994) Qualitative research methods for evaluating computer information systems, in *Evaluating Health Care Information Systems: Methods and Applications*, J.G. Anderson, C.E. Aydin and S.J. Jay (Eds.), Sage, Thousand Oaks, CA, pp. 45-68.

Kelly, E. P. and G. S. Erickson (2005) RFID tags: Commercial applications vs. privacy rights, *Industrial Management + Data Systems*, 105(5/6): 703-713.

Kettha (2007) *Ministry Finalising Draft of Personal Data Protection Bill*, Ministry of Energy, KL.

Kowlessar, G. (2012) *Warner: e-passports by 2017*. http://guardian.co.tt/news/2012-12-06/warner-e-passports-2017 accessed 04 March 2013.

Kurtz, L.A. (1998) The invisible becomes manifest: Information privacy in a digital age. *Washburn Law Journal* 38: 151-174.

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

Laudon, K. and Laudon, J. (2012) *Management Information Systems*, 12th Edition. Prentice Hall.

Lin, C.-Y., 2009. An Empirical Study on Organizational Determinants of RFID Adoption in the Logistics Industry. *Journal of Technology Management & Innovation* 4, 1-7.

Masnick, M. (2003) Wal-Mart Cancels RFID Smart-shelf Trial, in *Techdirt*. http://www.techdirt.com/articles/20030709/1138246.shtml accessed 04 March 2013.

McDonagh, M. (2002) E-Government in Australia: the challenges to privacy of personal information, *International Journal of Law and Information Technology*, 10:(3): 327-343.

Metro AG (2004) *The use of RFID in the Future Store in Rheinberg'*, http://www.future-store.org/servlet/PB/menu/1002376_l2/index.html accessed 04 March 2013.

Moroz (2004) *Understanding Radio Frequency Identification (RFID)*. http://www.rfidcanada.com/rfid.html, accessed 04 March 2013.

Murray, C. J. (2003) Privacy Concerns Mount Over Retail Use of RFID Technology, *Electronic Engineering Times*. http://eetimes.com/electronics-news/4046620/Privacy-concerns-mount-over-retail-use-of-RFID-technology, accessed 04 March 2013.

Ohkubo, M., Suzuki, K. and Kinoshita, S. (2005) RFID privacy issues and technical challenges, *ACM*, 48(9): 66-71.

Pavlou, P.A. (2011) State of the information privacy literature: where are we now and where should we go, *MIS Quarterly* 35(4): 977-988.

Patton, M. Q. (1999) Enhancing the quality and credibility of qualitative analysis, *Health Services Research* 34(5): 1189-1208.

Peslak, A. R. (2005) An ethical exploration of privacy and radio frequency identification, *Journal of Business Ethics* 59(4): 327-345.

Plos, T. Aigner, M., Baier, T., Hutter, M., Plos, T. and Wenger, E. (2012) Semi-passive RFID development platform for implementing and attacking security tags, Inter*national Journal of RFID Security and Cryptography (IJRFIDSC)*: (1:1/2): 16-24.

Poirier, C.C. and McCollum, D. (2006) *RFID Strategic Implementation and ROI: a practical roadmap to success*, J. ROSS Publishing.

Privacy International (2006) 2006 International Privacy Survey: Ranking by Country, *Privacy International*, http://www.privacyinternational.org/survey/phr2005/aboutphrtable.pdf accessed 04 March 2013.

RFID Journal (2005) What is RFID? *RFID Journal*, http://www.rfidjournal.com/articles/view?1339

Saunders, L. (2008) ID Cards for Australian?,The Drum Opinion. *ABC News*. http://www.abc.net.au/unleashed/31898.html accessed 04 March 2013.

Seidman, I. (2005) *Interviewing as qualitative research*, Third ed. Teachers College Press.

Siltaoja, M.E. (2006) Value priorities as combining core factors between CSR and reputation – A qualitative study, *Journal of Business Ethics* 68(1): 91–111.

Smith, H.J., Milberg, S.J. and Burke, S.J. (1996) Information privacy: measuring individuals' concerns about organizational practices, *MIS Quarterly*, 20(2): 167-196.

Sutanto, J., Palme, E., Tan, C.-H. and Phang, C.W. (2013) Addressing the personalization-privacy paradox: An empirical assessment from a field experiment on Smartphone users, *MIS Quarterly*, 37(4): 1141-1164.

Tedjasaputra, A. (2006) *MyKad: Technology for Whom*? http://www.rfid-asia.info/2006/07/mykad-technology-for-whom.htm accessed 04 March 2013.

Thiesse, F. (2007) RFID, privacy and the perception of risk: a strategic framework. *The Journal of Strategic Information Systems* 16, 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*, Melbourne University.

U.S. Congress (1995) Directive 95/46/EC of the European Parliament and of the Council, *Official Journal of the European Communities*.

U.S. Congress (2002) *One Hundred Seventh Congress of the United States of America*, edited by U.S Congress. Washington.

Vaudenay, S. (2006) RFID privacy based on public-key cryptography, in *Information Security and Cryptology – ICISC 2006*, Lecture Notes in Computer Science; Springer, 4296: 1-6.

Violino, B. (2005) What is RFID?, *RFID Journal*. http://www.rfidjournal.com/articles/view?1339 accessed 04 March 2013.

Welsh, E. (2002) Dealing with data: Using NVivo in the qualitative data analysis process. *Forum: Qualitative Social Research* 3.

Whiting, R. (2003) RFID backers, privacy advocates seek common ground, *Information Week* (11:17). http://www.informationweek.com/rfid-backers-privacy-advocates-seek-comm/16100902 accessed 04 March 2013.

Wikipedia (2009) *Identity Document*.http://en.wikipedia.org/wiki/Identity_document accessed 04 March 2013.

Wu, N., Nystrom, M., Lin, T. and Yu, H. (2006) Challenges to global RFID adoption. *Technovation* 26(12): 1317-1323.

Zikmund, W. G., Babin, B., Carr, J. C. and Griffin, M. (2010) *Business Research Methods*. Eighth Edition. Cengage Learning: Canada.