Building trusted national identity management systems: Presenting the privacy concern-trust (PCT) model

Adjei, Joseph K.; Olesen, Henning

Publication date:
2012

Document Version
Early version, also known as pre-print

Building Trusted National Identity Management Systems:

Presenting the Privacy Concern-Trust (PCT) Model

Joseph Kwame Adjei & Henning Olesen
Center for Communication, Media and Information Technologies (CMI)
Aalborg University Copenhagen
A. C. Meyers Vænge 15, DK-2450 Copenhagen, Denmark
e-mail: {adjei,olesen}@cmi.aau.dk

***Abstract*—This paper discusses the effect of trust and information privacy concerns on citizens' attitude towards national identity management systems. We introduce the privacy-concerns-trust model, which shows the role of trust in mediating and moderating citizens' attitude towards identity management systems. We adopted a qualitative research approach in our analysis of data that was gathered through a series of interviews and a stakeholder workshop in Ghana. Our findings indicate that, beyond the threshold level of trust, societal information privacy concern is low; hence, trust is high, thereby encouraging further institutional collaboration and acceptance of citizens' informational self-determination.**

Keywords-Identity Management; PCT Curve; Privacy Concern; Trust; Trusted Identities.

I. INTRODUCTION

Although digital Identity Management (IdM) is fundamental to electronic government, globally, its implementation and adoption by citizens usually presents complex issues for its many stakeholders. The complexity has been attributed to the fact that it transcends technological issues as well as policy, legal, institutional, and economic aspects of society. The complexity is also compounded by the rate, at which standards and technological solutions become obsolete; the flexibility and ease of collection, use, dissemination of data; and the increased link-ability of information to the data subject. This raises the potential for privacy concerns [1].

Ironically, previous privacy research has shown that individuals disclose personal information in exchange for some economic or social benefit subject to the "privacy calculus", an assessment that their personal information will subsequently be used fairly, and that they will not suffer negative consequences [2]. Moreover, where individuals can exercise some degree of control over data collection and use; information is collected in the context of an existing relationship; the information collected or used is relevant to the transaction; and they believe the information will be used to draw reliable and valid inferences about them; citizens are less likely to raise concerns. Unfortunately, this is usually not the case. These phenomena often occur without direct involvement or control of the data subjects.

Governments in many countries have implemented some form of identity management as a critical enabler of government to citizens' interactions, and in facilitation of business transactions. Unfortunately, the costs of implementations are usually not matched by the benefits and citizens' adoption of the expected or improvement in public services. This makes it difficult for governments to justify the implementation, since it often leads to embarrassment [3, 4].

In spite of its use being lower than expected, identity management can play a leading role, if the factors that affect its takeoff are properly addressed. Trusted identities ecosystems have been found to be very critical to the success of digital IdMS. This research focuses on understanding the key stakeholder concerns on information privacy in regards to the collection, storage, use, and transmission of personal identity information [5], and how such concerns should be addressed to ensure trusted identities.

The rest of the paper is organized as follows; the next section discusses the theoretical background for trust and privacy concerns, followed by a description of our research design and methods. We then discuss our findings from the stakeholder workshop and the interviews. We present our conclusions and recommendations for further studies in the final part of the paper.

II. THEORETICAL BACKGROUND

The growing deployment of innovative systems for collecting, processing, and sharing personally identifiable information places data subjects in a vulnerable situation and has propensity to undermine confidence in identity management systems. A 2012 Europe-wide survey [6] revealed that online users are naturally concerned about risks in online transactions, and that users are not in control of their personal information disclosed on the Internet. The survey also revealed that users employ a variety of offline and online methods to protect their identity; 62 % of users better understand how to protect their identity in the offline transactions using data minimization techniques, whilst 90 % trust national institutions and banks more than Internet service providers and e-shops [6]. Such observations cannot be true in many developing countries.

In developing countries many of the electronic government projects are viewed with suspicion with very low level of trust in the institutions that manage credentials. The source documents required for proofs of identities, i.e., civil registration systems are often unreliable [7] due to several instances of multiple registrations and enrolment of unqualified people. Businesses, usually, have difficulties in verifying the authenticity of credentials individuals presented for access to services. Credentials can in many instances only be

 ISBN: 978-1-61208-232-5

verified manually, resulting in undue delays and customer frustration with its attendant privacy information implications.

A. Information Privacy Concerns

The issue of privacy is generally based on cognitive perceptions rather than on rational assessments. Privacy concern has been used as a key privacy construct by researchers [8, 9]. Smith et al. [10] developed the concern for information privacy (CFIP) model for operationalizing privacy concerns based on data collection, errors, secondary use, and unauthorized access to information or invasion. Collection, use and transmission of personal information by identity providers and relying parties must in principle be based on tacit or explicit consent by service providers to protect the interest of data subjects [2]. Citizens, therefore, become apprehensive, when their interests are not observed, or the perceived risk of the abuse exceeds the benefits derived from such implied social contracts.

These tensions between organizational use of personal information and societal information privacy concern are very topical in privacy research [11]. Previous studies have defined privacy as *the ability of an individual to exercise some degree of control of the access that others have to their personal information* [12]. Privacy is at risk, if individuals are unable to exercise control over their personal information during social interactions and business transactions [13, 14], and it is therefore disheartening for privacy-aware citizens to find out that inaccurate, out-dated, excessive or irrelevant data about them are stored by others.

Information privacy concerns can be categorised as

- *Illegitimate use of information* [10], *and*
- *Secondary use of personal information without the consent of the data subject, for purposes outside the primary reason for data collection* [1].

Therefore, it is imperative that organizations develop information practices that address the perceived risks and citizens concerns in order to project an innate trust [15, 16]. Although privacy concerns are almost always measured at an individual level of analysis, societal concern (overall privacy concerns of a nation) should reflect the concerns of its citizens and organizations [17, 18]. Various governmental interventions like regulations and controls are implemented to address societal information privacy concerns. Although Bélanger & Crossler [17] and others have discussed the privacy concern, there is still a need to clarify *how privacy concern and trust affect each other within the context of identity management*. This is one of the objectives of this study.

B. Trust

Trust plays an important role in societal discourses and attitudes towards electronic identification systems. Due process requires that organizations apply best practices in data acquisition and also strive to prevent illegitimate access by others to personal data in their custody. Bhattacharya et al. [19] describes trust as having a multidimensional construct and defined trust as an expectancy of positive or non-negative outcomes that one can receive based on the expected action of another party in an interaction characterized by uncertainty [19]. Broadly, trust is considered as a firm belief in the reliability, competence, qualification, ability, strength, integrity, truthfulness, honesty, sincerity, and loyalty of the other party to transaction or interaction [20].

In their study on "an alternative model of trust", Mayer et al. [15] modelled the concept of trust by categorizing the key attributes of trustworthiness as the trustees' ability to fulfil the trusting action, the benevolence of trustees' intentions, and their integrity [15, 21]. Their definition was based on one person's beliefs about the characteristics of another person. In effect, trustworthiness can be operationalized using these three attributes of the trustee. Ability signifies competence or perceived expertise, business sense and judgement. Consistency, fairness and reliability describe integrity, whereas loyalty, openness and availability signify benevolence [15, 16]. These attributes are important determinants of the success of IdMS, since it can affect the usage behaviours of the systems.

A trust relationship is made up of three elements – the truster, the trustee, and the context in which trust is conferred [20]. Trusters are the citizens and relying parties, the trustees are the credential issuers and service providers, and the context is an IdMS or the electronic identity card scheme.

Perception of trust can be either due to the technology or the institutions [22]. A low citizens trust in credentials issuers and IdMS will be a major disincentive to accept the IdMS, since there is lack of identity assurance [23]. Such lack of trust can lead to unfavourable outcomes of the IdMS. Likewise, a low trust in credential issuers coupled with a high trust in the technology leads to a situation, where citizens might use technology as a competitive tool against the unpredictable and sporadic results. In such a scenario the IdMS will be viewed with suspicion and cynicism by the citizens [24, 22].

C. Relationship Between Trust and Privacy Concern

Various studies have established a relationship between trust and people's willingness to forgo their privacy concerns [25, 26]. What is not certain is the nature of the relationship between privacy, trust and societal attitude towards identity management systems. Trust is known to be a mediator between privacy concerns and behaviour [26, 27]. Thus, trust (the mediator) is what explains the effect that privacy concern (independent or predictor variable) has on societal attitude (the dependent or criterion variable). For instance, a correlation between income and cancer might be explained by a correlation between income and smoking (the mediator), and then between smoking and cancer. Thus, according to mediation models, privacy has little or no direct effect on behaviour; instead any effect can be explained by the links between privacy and trust, and then between trust and behaviour.

 ISBN: 978-1-61208-232-5

The relationship between privacy concern and trust can also be explained using the concept of moderation [28]. Moderators are variables that affect the directions and strengtsh of a relationship between an independent and a dependent variable [28]. Thus, in the case of privacy and trust, where there is high trust, privacy concern exerts an influence on behaviour, while in low trust environments privacy concern may have a negligible impact on behaviour, since behaviour is limited by the lack trust. This study explains mediator and moderator relationships between privacy concerns, trust and citizens attitudes towards national identity management systems.

D. Modelling Identity

Wilton [29] described digital identity as the relationship of identity between a person at the time of enrolment, and a person at the time of authentication [29]. Thus, identity is not just a snapshot of a person, but part of a process from enrolment and credential issue to credential presentation, authentication and revocation [29]. When such a process is not followed or abused, citizens become concerned and lose confidence in the system or the identity service providers.

E. Privacy Concern-Trust Curve

Generally, societal interactions and business relationships begin from a low level of trust (distrust) and high privacy concern. With disclosure of more information, strong institutional cooperation and user awareness, users are able to exercise some degree of user control over their personal information, resulting in the establishment of a certain level of trust. Thus, citizens become more empowered and revise their negative perceptions about the IdMS and identity service providers. This establishment of trust reduces the initial privacy concerns. Thus, a high privacy concern is associated with low level of trust, and reduction in privacy concern results in an increase in trust. In other words, the mediating and moderating effect of trust can result in either a negative or positive societal attitude changes towards IdMS.

The qualitative relationship between trust and privacy concern is shown in Fig. 1. A certain threshold level of trust must be overcome, before the citizens are ready to open up for interaction. The figure also shows that absolute trust or zero privacy concern is not possible within a trusted identities environment, and hence the curve can only asymptotically approach the two axes. The purpose of the trust framework therefore is for society to establish the framework that can overcome the trust threshold. Beyond this level, trust and privacy is adequate to encourage more collaboration, creation of new identity-based services, institutional collaboration, etc.

III. RESEARCH DESIGN AND METHODS

This study entailed two main phases – an exploratory phase, which saw the development of the model based on literature, and a qualitative based confirmatory phase, which was used to evaluate the model. The conceptual model on the basis of theoretical considerations is part of an on-going research project that seeks to present a reliable and valid instrument for measuring trusted identities ecosystem. The exploratory phase of the study was organized in line with two-step approach for operationalizing constructs and identifying measures [30]. Due to the multi-stakeholder nature of trusted national identities, we decided to adopt a research approach that engages the key actors and hence a qualitative methodological approach was deemed the most appropriate means for data collection from a societal perspective [31, 32]. We also applied the concepts of Interpretative Phenomenological Analysis [33] in our data analysis because of its usefulness in understanding the experiences of individuals. The overarching research question was *"what are the key requirements for crafting a trusted identities ecosystem"*.

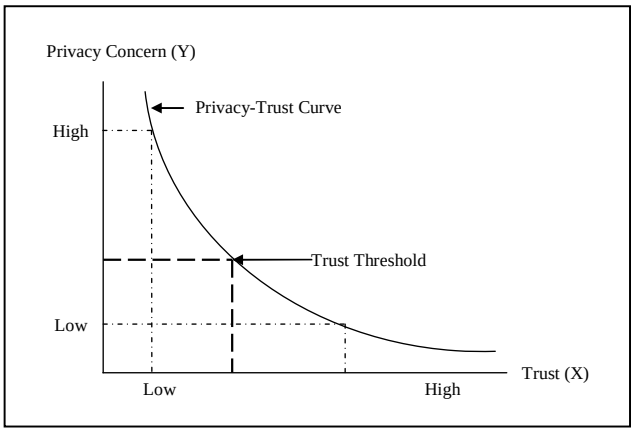

Figure 1. Qualitative relationship between privacy concern and trust.

A. Stakeholder Workshop

Given the societal level of analysis, a stakeholder workshop was organized in Accra, Ghana. All the major stakeholders involved in the collection, storage use and issue of identity were represented, including Registrar of Births & Death, The Passport Office, Driver and Vehicle Licensing Agency (DVLA), National Identification Authority (NIA), National Health Insurance Authority (NHIS), Electoral Commission (EC), Ghana Revenue Authority, financial institutions and identity-related businesses, academic institutions, national institutions and non-governmental organisations involved in civil right advocacy, and the general public. The identification challenges in Ghana are considered to be typical of many developing countries.

During the workshop participants were offered the opportunity to discuss a number of prepared questions and scenarios. To inform discussions, participants listened to presentations on various aspects of trust, privacy and secondary uses of personal information. The presentations also highlighted the key concepts of trusted identities and the policy, technological and regulatory implications as well as related IdMS research and practices in OECD countries [34, 35]. The ideal situation as illustrated on Figure 2 was used to explain the benefits of trusted identities.

Some of the discussion questions were:

 ISBN: 978-1-61208-232-5

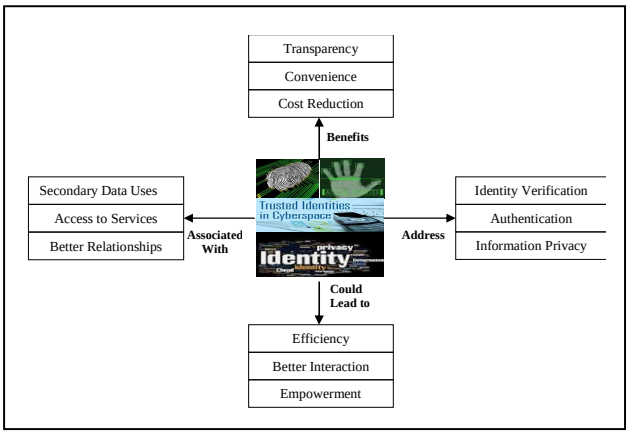

Figure 2. Dimensions of Trusted Identity Management Systems.

1. *What are the potential benefits and risks regarding the secondary uses of personal information?*
2. *What are the major challenges in relying on existing credentials presented for access to services?*
3. *How can institutional cooperation be encouraged given the conflicting regulations?*
4. *What attributes does citizens look for before trusting organizations with respect to secondary use of personal information?*
5. *What can be done to address issues arising from inappropriate use and/or exploitation of personal information?*
6. *What regulations, legislation, and/or policies are needed to address the evolving challenges?*

B. Interviews

A series of stakeholder interviews were conducted before and after the workshop. The pre-workshop interviews were made to identify the key issues and challenges from different perspectives. This helped in choosing and phrasing the discussion questions for the stakeholder workshop. The follow-up interviews were conducted to clarify some of the points raised during the workshop to solicit for further information. Interviewees included the officials of identity issuers, policy makers, journalists, private businesses involved in identity verification, and identity card manufacturers.

C. Transcription and Coding

Although raw data can sometimes be of interest in research they do not usually help the reader to understand the world under scrutiny and participants' views without a systematic analysis to illuminate the situation under investigation [36]. Transcripts were thus initially coded to aid meaningful analysis. Data coding, which is an important part of analysis, involves subdividing data into chunks of varying-sized words, phrases, sentences or whole paragraphs, and assigning categories [37]. Thus, codes are labels for allocating units of meaning to descriptive or inferential information compiled during a study. One of the key objectives of our coding approach is to identify relevant examples of the phenomena and analysis of the phenomena tp discover distinct patterns, differences and commonalities [37].

Transcript of the workshop discussions and the interviews, in the form of audio-visual recordings, interview notes and summary of discussion sessions, were produced by the authors. The introductory background of speakers and interviewees were, however, included for coding and analysis purposes. This was meant to maintain speaker anonymity. No attempt was made to identify speech patterns, since that was not the focus of our research. The nature of the discussions and interviews was such that initial coding would not have been helpful since participant interviewees were from diverse backgrounds, and opinions were varied. Each of the transcripts was coded on the basis of the background of the various speakers, since each of the participants and interviewees were told to introduce themselves before speaking. This served as basis for coding and sub-categorization of the transcript.

IV. DISCUSSION OF FINDINGS

A. Societal Concerns

Comments and statements made by participants during the interviews and workshop revealed a number of societal concerns and the various sources of them. Some of the concerns are listed below:

- *"The identity agencies are only there to please their political party and not because they are skilled".*
- *"If the electoral commission knew what they are doing, why will they opt for a biometric system without a means of verification"?*
- *"The information on the National Identification Authority website is so scanty that I have no idea what is going on."*
- *"I wonder if the officials of the identification agencies read our emails or even if the emails get to the organisations in the first place, because they never respond to emails sent to addresses they have provided".*
- *"If I have a problem, I have no idea how to reach them by phone or on the Internet, except if I walk to their head office"*
- *"I do not know the use of all the information collected by many of the identification agencies. For instance, I do not understand, why my actual date of birth is stated on my driving license, when they could have simply stated that I am over eighteen or qualified to drive."*
- *"Since one can present different documents as proof of identity during voter registration or drivers' license acquisition, it gives room for multiple registrations."*

Such comments show the need for societal assurance that their opinions are taken seriously. In a situation, where citizens do not get responses for the concerns raised, it gives the impression that citizens are not involved in decisions that concern them. It is therefore important to empower citizens in order to generate commitment and contributions. In essence, when citizens' opinions are taken seriously, they feel

 ISBN: 978-1-61208-232-5

that they are involved in decision-making and empowered, resulting in increased trust [38, 39].

Moreover, recruitment of unqualified personnel shows a lack of ability and integrity, which are all key attributes of trustworthiness [15, 40]. This is also manifested in comments like

- *"I always read stories in the dailies about impersonation and people making fake documents especially passports and birth certificates; many of the officials are involved"*.

However, citizens would like to have informational self-determination - a sense of freedom to do what is interesting, personally important, and psychologically vitalizing [41]. Such concerns lead to distrust in government institutions and therefore very critical that the system for tracking vital source documents like birth and marriage certificates is improved. The key aspects of the civil registration that need to be made efficient include, birth, marriage and death registration.

B. Segregation of Personally Identifiable Information

Article 7.1 of the United Nations Convention on the Rights of the Child states that *"the child shall be registered immediately after birth and shall have the right from birth to a name, the right to acquire a nationality, and as far as possible, the right to know and be cared for by his or her parents"*. The birth certificate for instance contains the given name, surname (or family name), gender, date of birth, place of birth, and father and mother names. Given the importance of the birth certificate in the establishment of the core identity, its abuse in the form of multiple registration and registration of illegitimate people defeats its usefulness. If the birth registration system were to be strengthened, it could act as the basic document that all residents must rely on for initial registration.

The information on the birth certificate represents the 'Basic Identifier Set' (BIS) – information that can help identify a person and does not change over time [29]. Hence, the birth certificate can be a very useful document in addressing issues of multiple registrations, especially when individuals are made to use the number throughout life. In that case, enrolment of foreign nationals who reside in the country should be based on travel documents as part of the processing of residence permit.

Certain transactions requiring proofs of additional information might require credentials that show the individual's Personally Identifiable Information (PII) – additional information that is useful for identifying a person but may change over time, such as addresses, marital status, physical characteristics like height, hair/eye colour, or complexion [29]. The PII provides additional information that can typically not be found in the BIS. For border control purposes passport may be preferred more than a birth certificate. In other sector-specific transactions and interactions, other attribute data are necessary for effective identity verification. This kind of data is information that on its own might not be able to identify a person, but will provide important traces when linked to either the BIS or PII data, or when such data are aggregated over time and space (e.g. healthcare records, tax return information, driver's and vehicle licence, banking and insurance information. Given the sometimes sensitive nature of such information, e.g. health records, it might require additional level of security to avoid linkability to the BIS and PII. In essence, other attribute data are identity-related, albeit 'sector-specific',

C. Strong Focus on Identity and not Credentials

A common misunderstanding on the part of credential issuers and policy makers during the workshop was the equation of strong credentials to efficient identity management systems. This became apparent from statements like *"we have introduced biometric based ID cards that are difficult to forge"*.

There is, therefore, the need to move away from credentials towards unique identification. A credential such as a passport or driving licence typically includes some items from each of the three aspects of identity – the BIS, PII such as height, eye colour, and some sector-specific data such as entitlement to drive specific classes of vehicle, or visas indicating entitlement to enter a specific country. This is illustrated on Fig. 3.

A distinct feature of a credential is that it encapsulates attributes and entitlements in a reliably verifiable form. There is therefore the tendency to equate such documents as representing the identity of a person when in fact they might not be representative in a given context. For instance, passports and driving licences have historically been presented as foolproof documents loaded with the necessary information that can enable the holder to access services and for authentication purposes. This is not without drawbacks, since it is susceptible to revealing more information about the holder than is necessary in any given authentication context. Using a passport for proof of age will no doubt reveal the passport holder's name, place of birth and citizenship, and a driver's licence used for similar purpose can also reveal your date of birth and address.

A focus on identity will also make it easier to enforce policies appropriate to the data in question, particularly when different sector-specific data items entail different policy controls. For instance, entitlement to drive a vehicle may not be part of major privacy concern, whereas credit status will, hence data security policies could be segregated to address such data. On the other hand, since healthcare history and medical conditions are very sensitive, a different set of policies will apply. Graphically, one might think of this as the ability to segregate identity data into sector-specific segments and cater for discrete management policies by sector and data type (cf. Fig. 3). Thus, within a given data segment, assertions of identity ('the holder of this credential is XX') may make one kind of data security policy appropriate, while assertions of other attributes ('the holder of this credential has been treated for Repetitive Stress Injury') may require quite different policy treatment.

D. Application of Privacy Enhancing Tools

Various privacy-enhancing and minimal disclosure technologies have been tested that address the requirement not to reveal unnecessary details in transactions. For instance, the

 ISBN: 978-1-61208-232-5

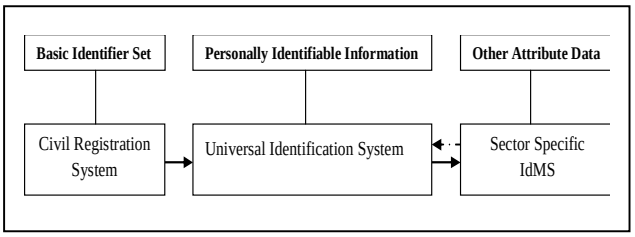

Figure 1. Personal Information and how it can be segregated.

touch2ID biometric application allows users to prove their age without storing or revealing extra details about the individual [42]. Similarly, the ABC4Trust project has released and tested guidelines for implementing attribute-based credential technologies focusing on trust, based on Idemix and U-prove technologies [43, 44, 45].

In an online context disclosure of excess data can be avoided. Credentials can realistically encapsulate just those data items, which serve to uniquely identify the holder (such as the BIS), as long as they provide a way of linking to the rest of the holder's personal data, which may be held elsewhere. In other words, the option now exists to make use of the distributed nature of networked computing, so as to allow much more flexible 'placement' of identity data of different types. This is valuable in terms of policy control, because it makes it possible to apply controls at the place where the data is held, rather than trying to enforce it wherever the credentials are verified.

E. Encouraging Trusted Environment

Trust is what moderates and mediates citizens' privacy concerns and attitudes towards IdMS. Thus, individuals are likely to engage in transactions, if their level of trust exceeds their personal privacy concern threshold, which is reached, when the potential benefits outweigh the risks. This threshold will always depend on the type of transaction and the amount of identifiable information revealed. For instance, transactions requiring the revelation of other attribute data might require a lower trust threshold. Thus, when positive steps (i.e., data minimisation) are taken to improve the IdMS, the moderation effect of trust will cause citizens to revise their attitude towards the IdMS, leading to more trust in the credential issuers and the technology and thereby moving down and to the right on the trust threshold. Similarly any negative actions on the part of credential issuers will increase the privacy concern and thereby causing a move upwards and to the left on the privacy trust curve. The trusted identities framework in the United States, where the interest of all stakeholders in the identity ecosystems are taken into account, is a clear step taken by the US government to increase trust [35].

V. CONCLUSIONS AND FUTURE RESEARCH

This paper discussed the issues and challenges associated with accountable management of personal identifiable information and the provision of more user control over personally information. The findings from this study suggest that information privacy concerns can affect the posture of society in relation to attitudes and preferences for regulatory environments and willingness to accept a particular identity management system [8, 18, 46, 26]. We also highlighted the relationship between information privacy concern and trust from a societal perspective, and its effect on trusted identity management systems.

Our findings show that unreliable civil registration system can be a major reason for such concerns. Given that the civil register is in many instances a key source document for credential acquisition, its unreliability leads to all kinds of credential abuses. Hence, governments especially in developing countries must focus on strengthening the civil registration system in order avert such abuses of personal identity information.

Our work clearly shows the two steps towards establishment of a trusted national framework, which are typical for the situation in many developing countries. Initially, trust is low and privacy concerns are high, because of poor implementations, but once the initial problems are identified and addressed, it is possible to pass a threshold level of trust, thereby reducing privacy concerns and paving the way for business and interaction. This is the point at which societal trust in Identity service providers is high enough to encourage institutional collaboration [22], and citizens' informational self-determination [41]. We also highlight the need for policy makers to categorise personal information in a way that will encourage secondary uses of personal information whilst ensuring that sensitive personal information is released only to legitimate people.

This study focused mainly on citizens' attitudes towards identification systems in Ghana and that poses a number of issues in terms of generalizability that will need to be tested. For instance, there are peculiar dynamics pertaining to every country and for that matter the inferences drawn might not be representative for all developing countries. Moreover, the use of a qualitative research approach also gives room for inferences that are not tested empirically, as is the case of quantitative research. In the future it will be interesting to examine quantitatively the relationship between trust and privacy concerns in relation to citizens' attitudes towards identity management systems.

REFERENCES

[1] M. J. Culnan, "How Did They Get My Name?: An Exploratory Investigation of Consumer Attitudes toward Secondary Information Use," *MIS Quarterly*, vol. 17, no. 3, pp. 341-363, 1993.

[2] P. H. Jos, "Social Contract Theory: Implications for Professional Ethics," *The American Review of Public Administration*, vol. 36, pp. 139-155, June 2006.

[3] E. A. Whitley and G. Hosein, "Global Identity Policies and Technology: Do we Understand the Question?," *Global Policy*, vol. 1, no. 2, May 2010.

[4] P. Seltsikas and R. M. O'Keefe, "Expectations and outcomes in electronic identity management: the role of trust and public value," *European Journal of Information Systems*, vol. 19, pp. 93–103, 2010.

[5] C. J. Bennett and C. D. Raab, The Governance of Privacy Policy Instruments in Global Perspective, Aldershot: Ashgate, 2003.

[6] W. Lusoli, M. Bacigalupo, F. Lupiañez, N. Andrade, S. Monteleone and I. Maghiros, "Pan-European Survey of Practices, Attitudes and

Policy Preferences as regards Personal Identity Data Management," European Commission JRC Scientific and Policy Reports, Luxembourg, 2012.

[7] WHO, "World Health Statics 2012," WHO Library Cataloguing-in-Publication Data, France, 2012.

[8] J. H. Smith and T. Dinev, "Information Privacy Research: An Interdisciplinary Review," *MIS Quarterly*, vol. 35, no. 4, December 2011.

[9] K. A. Stewart and A. H. Segars, "An Empirical Examination of the Concern for Information Privacy Instrument," *Information Systems Research*, vol. 13, no. 1, pp. 36-49, March 2002.

[10] H. J. Smith, S. Milberg and S. Burke, "Information privacy: Measuring individuals' concerns about organizational practices," *MIS Quarterly*, vol. 20, no. 2, pp. 167–196, 1996.

[11] R. Mason, "Four Ethical Issues of the Information Age," *MIS Quarterly*, vol. 10, no. 1, pp. 4-12, 1986.

[12] A. F. Westin, Privacy and Freedom, New York: Athenaeum, 1967.

[13] D. J. Solove, "A Taxonomy of Privacy," *University of Pennsylvania Law Review*, vol. 154, no. 3, pp. 477, 2006.

[14] R. Clarke, "Internet privacy concerns confirm the case for intervention," *Communications of the ACM*, vol. 42, no. 2, pp. 60-67, February 1999.

[15] R. C. Mayer, J. H. Davis and D. F. Schoorman, "An Integrative Model of Organizational Trust," *The Academy of Management Review*, vol. 20, no. 3, pp. 709-734, July 1995.

[16] J. K. Adjei and H. Olesen, "Keeping Identity Private," *Vehicular Technology Magazine, IEEE*, vol. 6, no. 3, pp. 70-79, September 2011.

[17] F. Bélanger and R. E. Crossler, "MIS Quarterly," *Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems*, vol. 35, no. 4, pp. 1017-1041, December 2011.

[18] P. A. Pavlou, "State of the Information Privacy Literature: Where are we now and whee should we go?," *MIS Quarterly*, vol. 35, no. 4, pp. 977-988, 2011.

[19] R. Bhattacharya, T. M. Devinney and M. Madan, "A formal model of trust based on outcomes," *The Academy of Management Review*, vol. 23, no. 3, pp. 459-472, July 1998.

[20] WP17, "D17.4: Trust and Identification in the Light of Virtual Persons," FIDIS, 2009.

[21] A. N. Joinson, "Privacy Concerns, Trust in Government and Attitudes to Identity Cards in the United Kingdom," *Proceedings of the 42nd Hawaii International Conference on System Sciences*, 2009.

[22] T. S. Teo, S. C. Srivastava and L. Jian, "Trust and Electronic Government Success: An Empirical Study," *Journal of Management Information Systems*, vol. 25, no. 3, pp. 99–131, 2008.

[23] S. J. Crosby, "Challenges and Opportunities in Identity Assurance," March 2008. [Online]. Available: http://www.hm-treasury.gov.uk/media/6/7/identity_assurance060308.pdf.

[24] S. Srivastava and T. Teo, "Citizen trust development for e-government adoption: Case of Singapore," in *Ninth Pacific Asia Conference on Information Systems*, Bangkok,, 2005.

[25] M. J. Culnan and P. K. Armstrong, "Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation," *Organization Science*, vol. 10, no. 1, pp. 104-115, 1999.

[26] N. K. Malhotra, S. S. Kim and J. Agarwal, "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model," *Information Systems Research*, vol. 15, no. 4, pp. 336-355, 2004.

[27] J. Nickel and H. Schaumburg, "Electronic privacy, trust and self-disclosure in e-recruitment. In extended abstracts on Human factors in computing systems," in , New York, USA, 2004.

[28] R. M. Baron and D. A. Kenny, "The moderator-mediator variable distinction in social psychological research: Conceptual, strategic, and statistical considerations," *Journal of Personality and Social Psychology*, vol. 51, no. 6, pp. 1173-1182, 1986.

[29] R. Wilton, "Identity and privacy in the digital age," *International Journal of Intellectual Property Management*, vol. 2, no. 4, pp. 411 428, 01-01 2008.

[30] A. Burton-Jones and D. W. J. Straub, "Reconceptualizing System Usage: An Approach and Empirical Test," *Information Systems Research*, vol. 17, no. 3, pp. 228–246, September 2006.

[31] J. W. Creswell, Qualitative inquiry and research design: Choosing among five approaches, 2nd ed., Thousand Oaks, CA: Sage Publications, 2007.

[32] R. K. Yin, Qualitative Research from Start to Finish, New York: The Guildford Press, 2011.

[33] J. A. Smith, "Reflecting on the development of interpretative phenomenological analysis and its contribution to qualitative research in psychology," *Qualitative Research in Psychology*, vol. 1, no. 1, pp. 39-54, 2004.

[34] OECD, 2011. [Online]. Available: http://dx.doi.org/10.1787/5kg1zqsm3pns-en.

[35] NSTIC, "National Strategy for Trusted Identities in Cyberspace: Enhancing Online Choice, Efficiency, Security, and Privacy April 2011," The White House , Washington, 2011.

[36] T. Basit, "Manual or electronic? The role of coding in qualitative data analysis," *Educational Research*, vol. 45, no. 2, pp. 143-154, 2003.

[37] I. Dey, Qualitative Data Analysis A User Friendly Guide for Social Scientists, London: Routledge, 2005.

[38] A. Wilkinson, "Empowerment: theory and practice," *Personnel Review*, vol. 27, no. 1, pp. 40-56, 1998.

[39] WHO, "WHO User empowerment in mental health – a statement by the WHO Regional Office for Europe," WHO Regional Europe, Copenhagen, 2010.

[40] R. Hardin, "The Street-Level Epistemology of Trust," *Politics & Society*, vol. 21, no. 4, pp. 505-529, 1993.

[41] E. Deci, J. Connell and R. Ryan, "Self-determination in a work organization," *Journal of Applied Psychology*, vol. 74, no. 4, pp. 580-590, 1989.

[42] C. Evry, "Proof-of-age scheme prepares to expand across Wiltshire," 2010. [Online]. Available: http://www.wiltshiretimes.co.uk/news/inyourtown/wiltshire/8239556.Proof_of_age_scheme_prepares_to_expand_across_Wiltshire/.

[43] J. Camenisch, I. Krontiris, A. Lehmann, G. Neven, C. Paquin, K. Rannenberg and H. Zwingelberg, "Architecture for Attribute-based Credential Technologies – Version 1," 2011.

[44] IBM_Research, "IDEMIX (Identity mixing) Project Overview," 2010. [Online]. Available: http://www.zurich.ibm.com/pri/projects/idemix.html. [Accessed 28th February 2012].

[45] Microsoft_Connect, "Microsoft U-Prove Community Technology Preview R2," 2010. [Online]. Available: https://connect.microsoft.com/site1188.

[46] F. D. Davis, "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology," *MIS Quarterly*, vol. 13, no. 3, pp. 319-340., 1989.

 ISBN: 978-1-61208-232-5