Secondary Uses of Personal Identity Information: Policies, Technologies and Regulatory Framework

Joseph K. ADJEI & Henning OLESEN
Center for Communication, Media and Information Technologies (CMI)
Aalborg University Copenhagen, Denmark

Abstract: Although personal identity information must primarily be used for protecting and promoting the physical needs of individuals, it has also become central to the business models of the digital age due to its use for other secondary purposes, resulting in various innovative identity management (IdM) solutions in OECD countries. Nonetheless, developing countries have still not been able to address basic identification challenges such as civil registration, real-time credentials verifications, etc. This paper discusses a means of communicating identity-related concepts to policy-makers, technologists, credential issuers and other stakeholders by addressing core issues relating to secondary use of personal information. The results of a stakeholder workshop in Ghana on secondary use of personal information are presented by stating the core issues and recommendations. We propose the adaptation and application of existing IdM research and experiences from OECD countries to deal with issues involved in using personal information for secondary purposes.

Key words: identity, identity management, personal information, secondary use, trust, privacy.

Technological advancements have paved the way for fast, easy and relatively cheap collection, aggregation and analysis of large volumes of data by third parties, with little or no involvement of the data subject [1] (MALHOTRA, KIM & AGARWAL, 2004; BÉLANGER & CROSSLER, 2011). At the core of these developments is the commoditisation of personal information, which has become a key component of modern business models. Parties in business transactions and social interactions usually rely on unique credentials [2] for proofs of identity, which sometimes are unrelated to the primary purpose of the credentials. Such secondary uses of personal information are necessary in

[1] Data subject is the individual to whom personal data relates.

[2] Credential is a generic term that can apply to both paper documents like Passports or Birth Certificates, and non-paper based objects such as smartcards and other tokens.

various jurisdictions, because the majority of business transactions and social interactions entail various forms of identity verifications and identity assurances. For instance, passports are primarily issued to aid border control, but sometimes might be required by banks or car rental agencies as proof of identity. Incidentally, such personal information usage also presents complex ethical, technological and policy challenges, which usually border on privacy, trust and security. These challenges have played a significant role in preventing access to and expansion of personal identity information (or simply "personal information") uses for secondary purposes.

Research consortiums and technology business organisations in countries within the Organisation for Economic Co-operation and Development (OECD) have developed cutting-edge solutions for addressing both offline and online technological and regulatory issues in identity management systems (IdMS), e.g. U-prove (Microsoft_Connect, 2010), OpenID (RECORDON & REED, 2006), Idemix (IBM_Research, 2010), Touch2id (Evry, 2010), etc. These developments can aid successful or effective uses of personal information for secondary purposes. For instance, businesses can now instantly verify the authenticity of credentials presented by clients, whilst maintaining the privacy of the holder. Government agencies can rely on information in identity databases to offer targeted social services to citizens.

In developing countries identification problems continue to persist, although many different credentials and tokens are issued to citizens, sometimes at a huge cost to the state. In Ghana, for instance, several independent IdMSs have been implemented resulting in the distribution of many forms of credentials. National Identification Cards, Birth and Death Registration, National Health Insurance Cards, Biometric Passports, Biometric Driver's Licences, Biometric Voter's Identity Cards and Tax Identification Numbers (TIN) are some of the widely used credentials.

All the IdM projects have focused on physical verification by the issuer [3] or their agencies in fulfilment of their mandate, with little emphasis on secondary usage by third parties and online or internet-based transactions. Many of the projects are initiated by government agencies with little private sector participation. Moreover, there is a general lack of interoperability and institutional co-operation contributing to difficulty in verifying the validity of

[3] Issuer is an agency that is legally authorised to issue credentials, such as the National Identification Authority or Passport Office.

key source documents like birth certificates and identity credentials, multiple registrations, impersonation, etc. Coherent policies, standards and best practices for secondary uses of personal information have therefore become imperative as a result of the growing availability of technologies supporting secondary uses. Addressing the many challenges ultimately requires a national framework for secondary use of personal information that is in the interest of citizens. The issues raised inspired this study to organise a stakeholder workshop to promote national discourse on secondary uses of personal information and their attendant issues.

The objective of this paper is to provide a means of communicating identity-related concepts to policy-makers, technologists, privacy advocates and users. The paper also addresses core issues relating to what constitutes personal identity information and user concerns in relation to secondary uses of personal information. The rest of the paper is structured as follows: The subsequent section discusses the background for this work. We then proceed to a comprehensive literature review discussing primary and secondary uses of personal identity information, the issue of identity, identification and identity management systems, and the major concerns of secondary uses of personal identity information. Subsequently we introduce our methodology for the study. The results from a stakeholder workshop in Ghana and follow-up interviews are presented, followed by a summary and discussion of the findings from the study. We present our conclusions in the final section, making a case for further studies in connection with commercialisation of personal identity information.

■ Background

Research, development and implementation of identity management systems in OECD countries have progressively gone through many stages, and various models have emerged. Currently, IdMS discussions in OECD countries have moved beyond issues in relation to civil registration coverage of births, silo and federated IdM models to user-centric IdM, where many of the research efforts are focused on identity assurance (EnCoRe, 2012; CROSBY, 2008). Moreover, many of the issues in connection with offline credential presentation and verification have been largely addressed, leading to more emphasis on electronic identity management systems with attribute-based credentials for enhancing privacy and anonymity as the

research focus. Several pilot and real life solutions have been successfully tested (CAMENISCH, *et al*., 2011).

On the contrary, many developing countries have still not been able to deal with fundamental identification challenges, and undue emphasis is still on primary usage of tokens by credential issuers and on physical verification, with little room for identity assurance and real-time verification by third parties. Some of the identification challenges can be traced to the reliability of source documents like birth and death register. In Ghana, for instance, the birth registration coverage is 71% according to WHO 2012 Health Statistics Report (WHO, 2012). This situation hinders the reliability of identity tokens for secondary uses by businesses and government agencies.

Existing IdM initiatives in Ghana are heterogeneous and independently managed with little involvement of other government agencies and the private sector. The various identification databases are all in silos and used primarily by the credential issuers as a means of fulfilling their main objective – e.g. voters' identity card is for electoral purposes. If a citizen's status changes (e.g. name change due to marriage), or the citizen changes address, the necessary changes have to be made with all the credential issuers separately. Moreover, internet applications of such credentials have not been a priority, thereby all the credentials are mainly for physical verifications. For instance, if a credential is presented for services, the service providers have no formal means of verifying its authenticity in real-time. There are opportunities for application developers to collaborate with credential issuers to develop verification and authentication systems for business. One such scenario is a local business that has developed credential verification application for financial institutions based on the voter register. The major challenge in this regard is lack of clear policies on secondary uses of personal information.

■ Literature review

An important aspect of the study has been to review IdM-related publications in research journals, and IdMS research and development in OECD countries. The key research works studied were: OECD Digital Economy Papers on identity management, European Union research projects on Future of IDentity in the Information Society (FIDIS) (FIDIS, 2007), Privacy and Identity Management in Europe for Life (PrimeLife), and

Attribute Based Credentials for Trust (ABC4Trust [4]) (CAMENISCH *et al*., 2011); the Kantara Initiative (WILTON, 2008); United Kingdom based research project on Ensuring Consent and Revocation (EnCoRe, 2012) and the US government's National Strategy for Trusted Identities in Cyberspace (NSTIC, 2011). Our study also draws on key IdM and privacy-related articles from *MIS Quarterly* (BÉLANGER & CROSSLER, 2011; PAVLOU, 2011), The Seven Laws of Identity (CAMERON, 2005), and Privacy by Design (CAVOUKIAN, 2008). The authors also listened to and watched various podcasts on U-Prove (Microsoft_Connect, 2010), and Idemix (IBM_Research, 2010) to understand the state-of-the-art in privacy-preserving identity management systems. Unfortunately, there were not many IdMS-related research articles from developing countries.

Identity, identification and identity management

The issue of identity has been widely researched from the perspective of technical scientists, psychologists, sociologists, etc. From a mathematical perspective, Leibnitz defined identity on the basis of whether two things can be distinguished from each other (WILTON, 2008; FELDMAN, 1970). He postulated that two objects sharing similar characteristics like shape, extent, position in time and space, could be deemed to have or share the relationship of identity (FELDMAN, 1970). Likewise, in our day-to-day physical interactions and on the internet, we leave our footprint in the form of pieces of information about ourselves, which accrete in various ways as we interact online. A person's identity is regarded as a reflection of those things, which are generally known about them by the people with whom they interact (WILTON, 2008). Identity is therefore a part of a chain of events from enrolment and credential issue through to credential presentation and hence a process, rather than a state.

Identification on the other hand is the process of linking information with a particular person, thus the action of being identified (CROMPTON, 2004). If identification is a process, then the integrity of the identification process and its usefulness will depend on the following factors: the reliability of the registration processes, verification and enrolment; how difficult it is to duplicate or alter credentials; and the difficulty in verifying the link between the credentials themselves and the person presenting them. To meet such

[4] http://www.abc4trust.eu/

identification criteria, an efficient system for managing identity will be necessary. Identity management therefore consists of the processes and all underlying technologies for the creation, management and usage of identities and their attributes. In effect, identity management unduly focuses on credential issuers and identity service providers with its implication on trust and misinterpretation of secrecy as a means of privacy protection.

Measures aimed at working towards user satisfaction lead to more focus on identity assurance. Identity assurance is a consumer/user led concept that enables data subjects to prove or provide informational representation during a chain of events that can define who they are without the need for them being physically present (CROSBY, 2008). Identity assurance must be a key element in identity management since it offers mutual benefits to identity service providers and to citizens. An identity assurance scheme can address issues such as the amount and type of data stored and the degree to which this information is shared.

Personal identity information

Personal information has become central to the business models of the digital age; to the management of government and state institutions; and to people's everyday lives and relationships. Business organizations sometimes apply strategies aimed at personalising service delivery to customers by focusing on customer preferences in order to offer specialised services (ALATALO & SIPONEN, 2001). Such practices could offer customers convenience, efficiency and personalisation, which can contribute to repeat of purchases. This inherently requires collection of pieces of customers' personal data or attributes. Among others, this is one reason why there is the need to take a closer look at what constitutes personal information (ANDRADE, KALTCHEVA & WEITZ, 2002).

Personal information is any information that specifically identifies an individual (e.g. name, telephone number, e-mail address, or account number), or their location or activities, such as information about his or her use of a website, when directly linked to personally identifiable information. In his Onion Model (WILTON, 2008), Wilton uses the layers of an onion as an illustration to categorise personal information into three layers – the core, inner layer and the outer layer. Information that can uniquely identify an individual and does not change over time, (e.g. name, date of birth) was placed at the core. Information at the core is known as a Basic Identifier Set

(WILTON, 2008). The inner layer consists of information that is capable of being used for identification but susceptible to change over time, such as address, height, etc. The outer layer consists of information that cannot uniquely identify a person, except when combined with some other information or aggregated overtime, such as a person's transaction history and sector specific information like blood group and health status. In effect, personal information is any information describing a natural person or information that describes an identifiable individual (TRUBOW, 1992)

Primary and secondary uses of personal information

Information must generally be used for the purpose of protecting, promoting, or meeting the physical needs of an individual or to enable that individual to participate in social interactions or benefit from services. Such information usages are regarded as the primary purposes of collecting personal information. For instance, the primary purpose of a Voter ID card is for an individual to vote in an election and that of a passport is to facilitate border control. Many of the data protection regulations mandate that personal information gathered for one purpose may not be used for any other purpose without the specific, informed consent of the data subject (TRUBOW, 1992). However, in order to conduct business such as opening a bank account, banks sometimes require tokens like a passport as a proof of identity. Such a requirement by the bank is secondary to the original intention of passports and voter IDs.

Culnan conceptualised secondary uses of personal information as having two dimensions: (1) The information processing activity (acquisition, use, or transfer) and (2) The relationship between the consumer and the firm utilizing the information (existing customer or prospect) (CULNAN, 1993). Secondary use of personal information therefore implies collection and storage of information for purposes other than originally intended by the issuer of the credential, whether legitimate or otherwise. Access to and use of personal information can in principle pose a number of complex challenges. In effect, for secondary use of personal information to be legitimate, there must be an "implied social contract" (tacit or explicit consent by service provides to protect the interest of data subjects) between service providers and users (MILNE, 1993). Where there is a perception of breach of such confidentiality, it affects the trusting relationship that should exist between service providers and data subjects (SOLOVE, 2006). Given that technological developments make such breaches difficult to notice,

secondary use of personal information poses technological, policy and regulatory concerns in relation with the ability to collect, store, aggregate, link, and transmit personal information for legitimate purposes. Such challenges have generally been researched in information systems under information privacy.

Privacy, information privacy and privacy concerns

Privacy is a topic, which has been studied in many different ways due to its many dimensions (SMITH, MILBERG & BURKE, 1996). It has been described as a condition or a state in which an individual can be more or less inaccessible to others, either on the spatial, psychological or informational plane (WHITLEY & KANELLOPOULOU, 2010). From psychology literature, WESTIN (1967) described privacy as the ability of individuals to control the terms under which personal information is acquired and used. From a sociological viewpoint, privacy has been defined as individuals' ability to independently dispose of their roles according to their right of self-determination, and then to have confidence that third parties respect the intended separation of their roles (BISKUP & BRÜGGEMANN, 1988). Defining privacy as an individual's personal space, CLARKE (1999) categorized personal space into four dimensions – privacy of the person (concerned with the integrity of the Individual's body), privacy of personal behaviour, personal communications, and privacy of personal data. Recent research has merged personal communication and data privacy into what is referred to as information privacy, due to the increased digitalization of information and communications (BÉLANGER & CROSSLER, 2011; PAVLOU, 2011). Hence, information privacy refers to the claims of individuals that their personal data should generally not be available to others, and that, where data are possessed by another party, the individual must be able to exercise a substantial degree of control over the data and their use (BÉLANGER & CROSSLER, 2011).

Information privacy concerns are related to factors affecting a person's willingness to render personal information (DINEV & PAUL, 2006), engage in online transaction activity (PAVLOU, LIANG & XUE, 2007), and the attitude towards government regulation (MILBERG *et al*., 2002). Although individuals express privacy concerns, many are willing to trade-in their privacy for convenience. This so-called privacy paradox (NORBERG, HORNE & HORNE, 2007; ZALLONE, 2010; ADJEI & OLESEN, 2011) also reaffirms the need for a more measured treatment of personal information.

Thus, information privacy is not about secrecy, which is an intentional concealment of information and (or) a disposition toward the sharing of potentially inaccurate information (TRUBOW, 1992). OECD guidelines (OECD, 1980), and other national data protection laws address various aspects of information privacy concerns, such as; (1) The existence of record systems cannot be kept secret; (2) an individual must be able to "find out what information about him is in a record and how it is used"; and (3) an individual must be able to "correct or amend a record of personally identifiable information (SOLOVE, 2006).

BÉLANGER & CROSSLER (2011) observed that development of privacy tools and technologies is usually done in isolation of the actual users and for that matter their input are not reflected in the systems design. The research approach adopted in this study is to address such concerns and to ensure active user involvement in secondary uses of their personal information.

Figure 1 – Privacy and dimensions of privacy

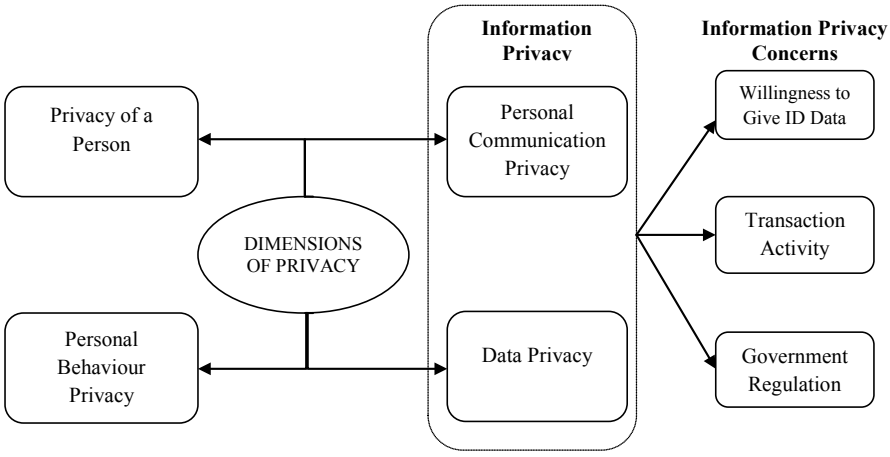

Figure 1 outlines the dimensions of privacy. Information privacy is related to personal communication privacy and data privacy. Major sources of concern are during data collection, data processing and data dissemination. Information privacy concerns affect individuals' willingness to provide information, their transaction activities and responses to government regulations.

■ Stakeholder workshop and interviews

This study adopted a qualitative methodological approach for data collection (YIN, 2009) resulting in a review of literature on the state-of-art on identity management, privacy issues in secondary use of personal information. The Interpretative Phenomenological Analysis (SMITH, 2004) approach was applied in the data analysis due to its reliability with respect to audio-visual contents, which is very common in focus group and workshop discussions. The issue of concern and for that matter the subject of the study was to find out what needs to be done in order to trigger successful or effective secondary uses of personal information within the context of an economy.

Stakeholder workshop

A stakeholder workshop was organised in Ghana on January 16, 2012, at Ghana Telecom University College (GTUC) in Accra. 75 participants were offered the opportunity to discuss a number of issues and listen to presentations highlighting issues concerning secondary uses of personal information. Letters were written to all the participants, and detailing the theme, agenda and activities for the day. The participants were made up of senior officials from national institutions involved in the collection and storage of personal information, such as 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. Also represented were senior officials of the major financial institutions, biometric and identity-related businesses, academic institutions, the media, non-governmental organisations involved in civil right advocacy, and the general public.

Ghana was selected as the research setting because the challenges faced by the economy with respect to identification and secondary uses of personal information are similar to those of other developing countries. Notable challenges include unreliable civil registration systems, electoral issues due to unreliable voters register, lack of identity management systems interoperability, etc. The workshop began with a statement from the Minister of Communication and a keynote address by the President of GTUC, who chaired the event. To inform discussions participants were given background information and copies of the discussion questions during a presentation on privacy and identity management. The presentation

highlighted the key concepts on identity management, including major policy, technological and regulatory issues and related IdMS research and practices in OECD countries. This was followed by another presentation on existing secondary uses of personal information for identity verification by financial institutions.

After the presentations participants shared their observations on the topic during the discussion session. Participants were also made to discuss the issues raised and share their experiences and their reservations. Where a particular issue or questions were sector-specific, the agencies concerned were given the opportunity to respond to such questions. Some of the discussion questions were:

- What are the potential benefits and risks regarding the secondary use of personal information?
- Who has the right to access personal information held by government agencies and for what purposes?
- What are the evolving public trust issues with respect to secondary use of personal information?
- Do citizens have the right to put constraints on the use of their personal information?
- What problems may develop as innovative technologies enhance the ability and ease of widespread personal data sharing for secondary purpose and commercial uses?
- What can be done to address issues arising from inappropriate use and/or exploitation of personal information?
- What regulations, legislation, and/or policies and procedures are needed to address these issues?

Interviews

A series of expert and stakeholder interviews were conducted after the workshop to offer stakeholders the opportunity to elaborate on some of the concerns raised by participants. It also offered interviewees the opportunity 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.

Transcription and coding

Transcripts of the workshop discussions and the interviews, in the form of audio-visual recordings, interview notes and summary of the discussion session were produced by the authors. The transcription mainly focused on speeches and statements made rather than who said what. This was meant to maintain speaker anonymity. No attempt was made either to identify speech patterns, since that was not the focus of our research. Each of the transcripts was coded on the basis of the introductory background of the various speakers, since each of the participants and interviewees were told to introduce themselves before speaking. This served as a basis for coding and sub-categorisation of the transcript. This style of coding and categorisation aided to consolidate the transcript into analytically distinct segments that could be examined together both within and between groups that covered the same concept (SMITH, 2004; WHITLEY & KANELLOPOULOU, 2010). For instance, statements like "Sorting out accurate birth register can reduce multiple registration", were felt to convey the same ideas as "many people present fraudulent birth certificate for IdMS enrolment". Hence, these two sets of codes were merged.

■ Results from the workshop and interviews

The organisation of the workshop, the presentations, application demonstrations, and questions and responses, prompted a lively discussion of the key issues, the available opportunities for secondary uses, and the major challenges. The analysis was also based on the major themes from the literature involving constant search through the codes and categories for contradictory and distinct claims and statements from the transcript (WHITLEY & KANELLOPOULOU, 2010).

The workshop enumerated many important issues associated with secondary uses of personal information. The issues were discussed from user, national and business perspectives. However there were areas where there existed commonality of opinions among participants. For instance, many of the participants were of the opinion that "organisations that make a conscious effort to maintain customer's privacy will in return gain customer loyalty". Highlights of the discussion are summarised in the following:

User perspective

From the user perspective, privacy and security of personal information, risk and cost associated with privacy abuses, government intervention policies and programs were of major concern. As an example, there are instances where "a person will go to a bank to withdraw remittances only to find out to their amazement that another person had already withdrawn the funds with that individual's personal details and sometimes fraudulent credentials". The panel discussed privacy implications of a real life scenario, where an identity issuer has authorised a private entity to operate a system for financial institutions to verify the authenticity of credentials, presented by customers. The key challenges to real time electronic information exchange were cost of bandwidth and power fluctuation, which are common in developing countries. Wilton's Onion model of Identity (WILTON, 2008) was also used to discuss, how personal information can be segregated to avoid linkability. It was observed that for users' interest to be served there was the need for emphasis on identity assurance (CROSBY, 2008; WHITLEY & KANELLOPOULOU, 2010)

Business perspective

Major discussion topics included the growing commercialization of personal information where there were several varied opinions. It became apparent that efforts should be made by government agencies to promote effective secondary uses. Panellists observed that there were not many opportunities for secondary uses in Ghana, a situation that is common in many developing countries, and hence the need for creation of a taxonomy of secondary uses of personal information. Two industry viewpoints provoked dialogue, one from the credential issuers, who think that third party verification is not their core business, and a second from the financial institutions, who need such verification to conduct transactions. Tables 1, 2 and 3 outline business, the key roles and responsibilities.

National perspective

The panel discussed the growing use of IdMS for national security, public health, social security, child protection and payment processing. These can only be realised if policy makers and credential issuers will see personal information not as matter of secrecy but something that, if well managed, can facilitate business transactions and a knowledge economy. Options for adaptation of various OECD research initiatives were discussed including roles and responsibilities of key stakeholders as shown in tables 1, 2 and 3.

For instance, the rules for obtaining user consent secondary uses, addressing civil registration issues, etc. There were diverse opinions regarding the most effective and practical approaches to accomplish this, and hence this is a subject for further discussion.

Table 1 – Typical secondary use scenario: key stakeholders, their interests and responsabilities

Typical Transactions	*Businesses*	*Consumers*	*Identity Issuer*
Online transactions	Business need information on customers and their transaction history	Consumers would like to apply for jobs or make online payment and to ensure privacy protection	Must ensure that credentials held by the right person
Transaction Negotiation	Businesses want prior knowledge of customer preferences.	Consumers would like to know if the seller or the transaction is genuine.	Must ensure real-time credential verification.
Identity Verification	Businesses want proof that customers are legitimate.	Customers need assurance that their privacy is not abused	Enforce minimum disclosure and data security policies
Payment Confirmation	Businesses want assurance that customers are credit worthy	Customers need a proof of total cost to avoid any hidden charges.	Would like to issue credentials that are easy to use
Payment Assurance	Businesses want assurance that customers will pay on due date.	Desires protection against disclosure of payment details and unauthorised deductions	Must ensure that systems are secure from abuse.
Order Fulfilment/ Delivery	Businesses need protection against customers' unjustified cancellation of order.	Customers would like to ensure that goods and services are delivered.	Must ensure that credential information is reliable.

■ Major findings and discussion

The discussion revealed the need for a paradigm shift with respect to ownership and control of personal information. The "identity" an individual seeks to assert is not their physical being as such, but rather an informational representation of the chain of life events that is defined by who they are. The particular events of relevance depend on with whom the individual is dealing and will lead to different entitlements. In that regard, attention must be focused on access to and control of personal information rather than data ownership. Focusing on data access and controls will ensure that appropriate policies for secondary uses of personal information will be developed since focusing on data ownership diverts attention from needed policies and practices. The workshop therefore recommended focus

on data access, control policies and practices as the best approaches to risk management and mitigation for secondary use of personal information.

Table 2 provides a summary of some of the key recommendations.

Table 2 – Recommendations for secondary uses of personal information

Issues discussed	*Recommendation*
Policy on secondary uses	Implement transparent policies and practices for secondary uses of personal information, taking advantage of available research and technologies.
Access to personal information	Focus on data access and control policies and practices for secondary use of data and not data ownership or secrecy.
Trusted identities	Ensure reliable civil registration.
Benefits and challenges associated with secondary use of information	Increase public education on benefits of secondary use of personal information.
Available secondary uses	Create a taxonomy of secondary uses of personal information and clarify its societal, public policy, legal, and technical implications

Privacy and trust emerged as two major issues; firstly, lack of understanding and inability to differentiate privacy from secrecy; and secondly, inadequacy of safeguard procedures that address user concerns in relation to secondary uses of personal information. In essence, citizens would like to be able to assert their identity with ease and confidence and hence they need such assurances (CROSBY, 2008). The workshop observed that lack of clear regulations (e.g. uses of data obtained via coerced or compelled consent) could result in the erosion of public trust. A taxonomy for identifying possible secondary uses of personal information is therefore required in order to clarify societal, public policy, legal and technical issues arising from secondary use of personal information.

Policy considerations

> "As long as we persist with a 17th century notion of national sovereignty, an 18th century judiciary and 19th century law enforcement, the 21st century will belong to organised crime." (Jeffrey Robinson [5])

[5] Jeffrey Robinson: writer on money laundering and organized crime.

Addressing the issues raised requires clearly defined policy initiatives. The following section outlines requirements for appropriate policies to provide high-level guidance for secondary uses of personal information, user empowerment, security, and privacy protection.

Interoperability

Policy issues in relation to IdMS interoperability have legal, business process and technical implications. The challenges are for credential issuers and service providers to articulate clear sets of policies containing a common set of elements, to enable comparison of those policies across organisations, to highlight areas of compatibility and to facilitate policy interoperability. At the legal level, there is the need for regulatory interoperability among various credential issuers in order to minimise regulatory complexities (OECD, 2011).

Information privacy and user empowerment

Many of the digital IdM solutions and privacy related principles like user control and consent, anonymity, (un)linkability, minimum disclosure, *etc.*, implicitly assume a certain level of user literacy. This is not always the case for all users (CAMERON, 2005; OECD, 1980). Public education and awareness programmes will play a major role in empowering users and fostering trust.

Security and trust

There is a need for development of consistent policies to ensure availability, confidentiality and integrity of personal identity data stored and exchanged since these are where user concerns emanates from. Inherent challenges in this regard are the constant availability of the systems and accuracy. Greater transparency in the enrolment and system use will increase citizens' trust in institutions.

Table 3 summarizes the identified responsibilities of the various stakeholders in order to promote secondary use of personal information.

Table 3 – Stakeholders responsabilities in promoting secondary use of personal information

Principles and guidelines	*Credential issuers*	*Service providers*	*Policy makers*
The Laws of Identity & Privacy by Design (PbD) Guidelines, etc.	Review existing IdMSs to ensure trusted identities	Develop easy to use privacy enhancing applications	Privacy audit of existing mainstream IdMS
Privacy Research Initiatives	Adopt and adapt attribute based privacy enhancing credentials	Develop minimum disclosure applications	Empower users by promoting awareness programmes
OECD Guidelines and Data protection laws	Implementation of interoperability policies	Focus on PbD & Training	Review policies to ensure process interoperability
Institutional Specific Laws	Identify conflicting areas	Report conflicting laws	Review laws to ensure legal interoperability

■ Conclusion and further research

Central to effective uses of personal information is an efficient civic registration system, a regulatory framework that encourages institutional collaboration, clear policies and guidelines that provide assurance of citizens' privacy and cost effective application systems. This is what the paper attempted to highlight by using the stakeholder approach and is considered its major achievement. The study has also helped to raise awareness of current technological developments and in IdMS and how developing countries can adapt and apply them. This call has been guided by the fact that application of Digital identity management is a process, rather than a state, the integrity of which depends on: how reliable were the initial processes of registration, verification and enrolment, and how hard is it to duplicate or alter the credentials used? (WILTON, 2008).

Moreover the use of the stakeholder workshop was as an attempt to bring together users and researchers, public and private sector organizations. It is a key methodological contribution and also a response to BÉLANGER & CROSSLER's (2011) call for closer collaboration between researchers, developers and users to ensure effective uses of privacy enhancing identity management systems.

Like many qualitative research methodologies a key limitation of our study is its lack of empirical testing of the claims compared to quantitative research. Also given that certain societal dynamics are peculiar to different

countries, care must be taken in generalizing the findings from our study to other countries.

A follow-up stakeholder workshop that combines focus group discussions to recommend practical solutions for secondary uses of personal information for commercial purposes is planned in the last quarter of 2012.

References

ADJEI, J. K. & OLESEN, H. (2011): "Keeping Identity Private", *Vehicular Technology Magazine, IEEE*, 6(3), 70-79.

ALATALO, T. & SIPONEN, M. T. (2001): "Addressing the personalization paradox in the development of electronic commerce systems", EBusiness Research Forum (eBRF), Tampere, Finland.

ANDRADE, E. B., KALTCHEVA, V. & WEITZ, B. (2002): "Advances in Consumer Research", *Self-disclosure on the Web: the impact of privacy policy, reward, and company reputation*, 29(1), 350-353.

BÉLANGER, F. & CROSSLER, R. E. (2011, December): "Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems", *MIS Quarterly* 35(4), 1017-1041.

BISKUP, J. & BRÜGGEMANN, H. H. (1988): "The Personal Model of Data: Towards a Privacy-Oriented Information System", *Computers & Security*, 7, 575-597.

CAMENISCH, J., KRONTIRIS, I., LEHMANN, A., NEVEN, G., PAQUIN, C., RANNENBERG, K. & ZWINGELBERG, H. (2011): "Architecture for Attribute-based Credential Technologies – Version 1", ABC4Trust.

CAMERON, K. (2005): "The Laws of Identity", from identityblog http://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf.

CAVOUKIAN, A. (2008): *The case for privacy-embedded laws of identity in the digital age*, Technical report.

CLARKE, R. (1999, February). "Internet privacy concerns confirm the case for intervention", *Communications of the ACM*, 42(2), 60-67.

CROMPTON, M. (2004): "Proof of ID Required? Getting Identity Management Right", Australian IT Security Forum.

CROSBY, S. J. (2008, March): "Challenges and Opportunities in Identity Assurance. From HM Treasury".
http://www.hm-treasury.gov.uk/media/6/7/identity_assurance060308.pdf

CULNAN, M. J. (1993): " 'How Did They Get My Name?': An Exploratory Investigation of Consumer Attitudes toward Secondary Information Use", *MIS Quarterly*, 17(3), 341-363.

DINEV, T. & PAUL, H. (2006): "Privacy Concerns and Levels of Information Exchange: An Empirical Investigation of Intended e-Services Use", *e-Service Journal*, 4(3), 25-60.

EnCoRe - Ensuring Consent and Revocation (2012). http://www.encore-project.info

EVRY, C. (2010): "Proof-of-age scheme prepares to expand across Wiltshire", *Wiltshire Times*. http://www.wiltshiretimes.co.uk/news/inyourtown/wiltshire/8239556.Proof_of_age_scheme_prepares_to_expand_across_Wiltshire/

FELDMAN, F. (1970): "Leibniz and 'Leibniz' Law' ", *The Philosophical Review*, 79(4), 510-522.

FIDIS. (2007): "Future of Identity in the Information Society", Deliverable-Report. D13.6: Privacy modelling and identity.

IBM_Research (2010): "IDEMIX (Identity mixing) Project Overview". http://www.zurich.ibm.com/pri/projects/idemix.html (retrieved 2012, 28th February

MALHOTRA, N. K., KIM, S. S. & AGARWAL, J. (2004): "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model", *Information Systems Research*, 15(4), 336-355.

Microsoft_Connect (2010): "Microsoft U-Prove Community Technology Preview R2", Microsoft Connect. https://connect.microsoft.com/site1188

MILNE, G. R. (1993): "Direct Mail Privacy-Efficiency Trade-Offs within an Implied Social Contract Framework", *Journal of Public Policy & Marketing*, 12(2), 206-215.

NORBERG, P. A., HORNE, D. R. & HORNE, D. A. (2007): "The Privacy Paradox: Personal Information DisclosureIntentions versus Behaviors", *The Journal of Consumer Affairs*, 41(1), 100-126.

NSTIC (2011): "National Strategy for Trusted Identities in Cyberspace: Enhancing Online Choice, Efficiency, Security, and Privacy April 2011", Washington: The White House. http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf (retrieved June 28, 2012)

OECD

- (1980): "From Guidelines on the Protection of Privacy and Transborder Flows of Personal Data". http://www.oecd.org

- (2011): "From Digital Identity Management for Natural Persons: Enabling Innovation and Trust in the Internet Economy - Guidance for Government Policy Makers". http://dx.doi.org/10.1787/5kg1zqsm3pns-en

PAVLOU, P. A. (2011): "State of the Information Privacy Literature: Where are we now and whee should we go?" *MIS Quarterly*, 35(4), 977-988.

PAVLOU, P. A., LIANG, H. & XUE, Y. (2007): "Understanding and Mitigating Uncertainty in Online Exchange Relationships: A Principal-Agent Perspective", *MIS Quarterly*, 31(1), 105-136.

RECORDON, D. & REED, D. (2006): "OpenID 2.0: a Platform for User-centric Identity Management", Second ACM workshop on Digital identity management (DIM'06) (pp. 11-16), New York, USA: ACM.

SMITH, H. J., MILBERG, S. & BURKE, S. (1996): "Information privacy: Measuring individuals' concerns about organizational practices", *MIS Quarterly*, 20(2), 167-196.

SMITH, J. A. (2004): "Reflecting on the development of interpretative phenomenological analysis and its contribution to qualitative research in psychology", *Qualitative Research in Psychology*, 1(1), 39-54.

SOLOVE, D. J. (2006): "A Taxonomy of Privacy", *University of Pennsylvania Law Review*, 154(3), 477.

TRUBOW, G. (1992): "Personal privacy and secondary-use dilemma (social aspects of automation)", *Software, IEEE*, 9(4), 73-74.

WESTIN, A. F. (1967): *Privacy and Freedom*, New York: Athenaeum.

WHITLEY, E. A. & KANELLOPOULOU, N. (2010): "Privacy and Informed Consent in Online Interactions: Evidence from Expert Focus Groups", Thirty First International Conference on Information Systems. St. Louis: AISeL.
http://aisel.aisnet.org/icis2010_submissions/126

WHO (2012): *World Health Statics 2012. France*, WHO Library Cataloguing-in-Publication Data.

WILTON, R. (2008): "Identity and privacy in the digital age", International Journal of Intellectual Property Management, 2(4), 411 428.

YIN, R. K. (2009): *Case Study Research: Design and Methods* (4th ed., Vol. 5), UK: Sage.

ZALLONE, R. (2010): "The Privacy Paradox or How I Learned to Have Rights that Never Quite Seem to Work", AAAI Spring Symposium Series, pp. 199-202, Palo Alto, California.