Analysis of Privacy-Enhancing Identity Management Systems

Adjei, Joseph K.; Olesen, Henning

Publication date:
2011

Document Version
Early version, also known as pre-print

Analysis of Privacy-Enhancing Identity Management Systems

Joseph K. Adjei and Henning Olesen

Center for Communication, Media and Information Technologies (CMI)
Aalborg University Copenhagen
Lautrupvang 1A, 2750 Ballerup, Denmark
E-mails: {adjei, olesen}@cmi.aau.dk

***Abstract*— Privacy has become a major issue for policy makers. This has been impelled by the rapid development of technologies that facilitate collection, distribution, storage, and manipulation of personal information. Business organizations are finding new ways of leveraging the value derived from consumer information. On the other hand, consumers have expressed concerns that their rights and ability to control their personal information are violated. Paradoxically, it appears that users provide personal data freely and willingly, as it has been observed on Facebook and other social networks. This study is an attempt to understand the relationship between individuals' intentions to disclose personal information, their actual personal information disclosure behaviours, and how these can be leveraged to develop privacy-enhancing identity management systems (IDMS) that users can trust. Legal, regulatory and technological aspects of privacy and technology adoption are also discussed.**

***Keywords*—Privacy, Trust, Identity, Identity Management**

I. INTRODUCTION

Incidences of cyber fraud and abuse of privacy on the Internet can have serious consequences for electronic business and the users' trust in performing online transactions. When security is breached, it also endangers user privacy and trust in institutions. Such security breaches have contributed to a growing desire for efficient and cost-effective measures in the design and administration of IDentity Management Systems (IDMS).

Several governmental and business initiatives seek to place the administration and control of identity information directly in the hands of individuals. These initiatives are aimed at curtailing security breaches and abuses of privacy in order to boost user confidence in online transactions and interactions. They require that individuals be given the right to exercise control over the collection, use, and disclosure of their personal information – their digital personae. Previous researches have proposed Fair Information Practice (FIP) principles, Privacy by Design (PbD) and The Seven Laws of Identity [1], [2], and [3]. These proposed frameworks and best practices seek to balance an individual's right to privacy with the organization's legitimate need to collect, use, and disclose personal information. Such attempts to give users the latitude to their digital identities are generally referred to as user-centric.

Unfortunately, researchers and developers of user-centric IDMS have mainly focused on making existing IDMS architectures interoperable, while privacy should actually be at the core of the IDMS design. Again, there is the perception that even though individuals advocate for their privacy, they have little or no reservations in releasing their personal information in social networks (e.g. Facebook).

This so-called "privacy paradox" is what motivates our study. Furthermore, many of the current initiatives are focused on online solutions and services in the digital world, but identity management also needs to take into account differences between users' behaviour in the physical and the digital world. The objective of this work is therefore to understand the major issues involved in the design of privacy-enhancing IDMS and contribute to improved framework and design principles for these.

The paper analyses existing international privacy regulations and the proposed standards and best practices in view of Technology Acceptance Model (TAM) [4]. The remaining part is divided into five sections. Section II contains definitions and concepts and gives a review of research on identity management, privacy and trust. In Section III, some of the major frameworks, initiatives and best practices are presented and compared. Section IV deals with privacy enhancing technologies for authentication and authorization, in particular U-Prove and OAuth. In Section V we present an updated framework and discuss the requirements and guidelines for realizing privacy-enhancing identity management, and finally, Section VI summarizes our finding and conclusions and give some recommendations for future studies.

II. IDENTITY MANAGEMENT, PRIVACY AND TRUST

The objective of this work is to understand the major issues involved in the design of privacy-enhancing IDMS. This is based on the premise that designing privacy enhancing technology is not just a technological problem but theoretical, social and regulatory dimension must also be addressed. The research problem then is "What factors must be considered in designing privacy-enhancing IDMS that address both online and offline identity management issues?". To address the research question we analysed the major privacy and data protection regulations, research initiatives, privacy-enhancing technologies in the light of technology acceptance model.

A. Identity and Identity Management

Identity in information systems consists of traits, attributes, and preferences, based on which an individual may receive personalized services. These services could be online, on mobile devices, or face-to-face (Liberty, 2004). In essence, identity has both physical and digital dimensions. Digital (or electronic) identity is therefore an electronic representation of a real-world entity or an online equivalent of an individual (Roussos, Peterson, & Patel, 2003). Traditionally, IDMS are run by organizations that control all mechanisms for authentication (establishing confidence in an identity claim's truth) and authorization (deciding what an individual should be allowed to do), as well as any behind-the-scenes profiling or scoring of individuals [5].

In this study, we adopt the Van Thuan (2007) definition of IDMS as *"consisting of processes, policies and technologies used to manage the complete lifecycle of user identities across a system and to control the user access to the system resources by associating their rights and restrictions".*

To ensure protection of privacy, security and provision of trusted services, different variations of IDMS were used throughout history to establish the basis for trade and governance by means of tokens and technologies, seals, coded messages, signatures, jewellery, etc. (3G_Americas, 2009). There has been a tremendous growth in in online government services, business transactions and social interactions via single sign-on (SSO) (Aichholzer & Strauß, 2009). Such activities require efficient and effective user identification and authentication, making IDMS very challenging. Clarke (1994) posits that identification is *"the association of data with a particular human being"*. Authentication is a process that results in a person being accepted as authorized to engage in or perform some activity (Whitley, 2009). Lips (2008) suggested a shift in focus towards analyses of the wider societal implications of IDMS implementation and related social design issues.

B. Concepts of Privacy

Privacy refers to the claim or right of individuals to exercise a measure of control over the collection, use and disclosure of their personal information. Westin (2003) described privacy concern as customers' apprehension over the acquisition and use of their personal data.

Until recently, personal identity and privacy were something of which each human being could exercise a reasonable degree of control [6]. With the advent of the Internet and high-speed communication technologies, it has become an illusion for users to assume physical control over the collection and use of their personal information since data can be mishandled. For example in many instances, users have little or no involvement the dissemination of their personal information. In essence, mishandled personal information puts individual's privacy interests at risk.

It is for this reason that governments must protect their citizens. Interestingly, many of the present privacy legislations in Europe were drafted on the basis of the Strasburg Convention of 1981 [6]. Therefore, legislation does not adequately assist in resolving contemporary privacy intrusion cases.

Furthermore, what constitutes personal information has comparatively widened due to increased usage of digital media for business and social interactions, e.g. user names, passwords, etc. Moreover, the concept of privacy has both collective and individual dimensions [7]. Hence, privacy cannot be conceptualised as autonomy from collective norms. This is what informs the debate on whether privacy protection is best approached on the basis that it is a private good or a common good [8]. The rights and obligations of individuals in many countries have therefore been weighed against the collective security and public safety goals – particularly in the USA and UK [8].

C. Concepts of Trust

Privacy concern has far-reaching effects on individuals' attitudes towards IDMS. Where there is the concern of vulnerability, people become apprehensive towards the systems. According to the Oxford Dictionary, trust is the belief that somebody or something is good, sincere, honest, etc., with no intention to harm or trick. There are different research positions on what constitutes trust and on the outcomes of trust [9]. In the literature, trust has been defined as the confidence in an exchange partner's reliability and integrity [10]. This confidence provides the basis for customers to believe in the reliability and integrity of organizations. It is one of the building blocks for information is sharing. Milne & Boza (1999) and Norberg et al. (2007) examined how privacy concerns are related to trust. They have suggested that increasing trust can mitigate privacy concern.

In Mayer et al. (1995) trust is conceptually distinct from the behaviours that may or may not reflect it. Without a clear distinction between the behaviours the difference between trust and similar constructs is blurred. For instance, Mayer et al. conceptualized trust as *the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other party will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party.*

Effectively, in a trustworthy relationship, individuals are motivated to share personal information freely with no fear of exploitation. Hence, trust can influence both positive and negative behaviour of people. This claim is shared by [11]. They observed that the basic ingredients of trust are: 1) dependence on the trusted party, 2) reliability of the trusted party, and 3) risk in case the trusted party does not perform as expected. This implies that trust requirements have direct correlation with risk exposure.

In the study conducted by Mayer et al., three important characteristics of trust were revealed: Ability, benevolence and integrity. Ability also implies competence or perceived expertise. Consistency, fairness and reliability were also used to have also used to describe integrity whereas loyalty openness and availability were used to describe benevolence. These trust characteristics are adopted in this study as the constructs of trust.

D. The Privacy Paradox

In many privacy scenarios, commercial interests seek to maximize the value of consumer information. For instance, many websites that provide useful information also require users to register in order to access the information. Even though individuals may be willing to part with personal information in order to realize the perceived benefits, many express concern about the violation of their rights and ability to control their personal information.

If we had perfect identity, security would not be an issue, just as systems with perfect anonymity will not present any privacy problem. In spite of the complaints, common use of

Facebook, Twitter, etc., indicates that consumers quite often freely release personal data in their interactions and business transactions [12]. This is referred to as "The Privacy Paradox" [12], [6]. Privacy paradox is the relationship between individuals' intentions to disclose personal information and their actual personal information disclosure behaviours.

An IBM 2008 survey suggests that individuals see a trade-off between the increased value of services and the consequent erosion in their privacy [13]. Consumers are on the one hand seeking for online experience devoid of fraud, cheaper and more conveniently delivered. Yet, there are fears that this could lead to an erosion of users' privacy. In essence, technology has a dual nature: User empowerment and raising security and privacy concerns.

E. Technology Acceptance Model (TAM)

Factors affecting technology adoption have been extensively studied in the Information Systems literature. Morris & Dillon (1997) posit that user acceptance is "the demonstrable willingness within a user group to employ information technology for the tasks it is designed to support". Notable research on adoption and diffusion of technology includes Innovation Diffusion Theory (Rogers, 1983), TAM (Davis, 1989) and the unified theory of acceptance and use of technology (UTAUT) (Venkatesh & Davis, 2000).

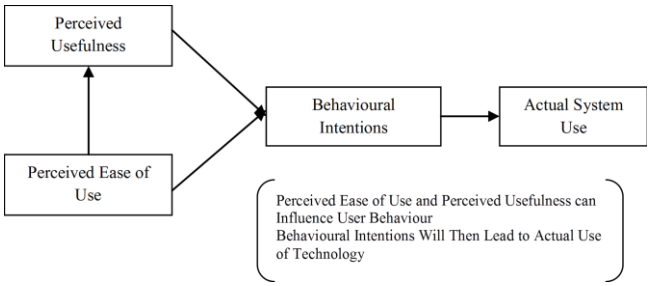

Fig. 1. Main elements of the Technology Acceptance Model *(Adapted from* [4]*).*

In Davis (1989) perceived usefulness (PU) and perceived ease of use (PEOU) were theorized to be fundamental determinants of behavioural intentions to accept or reject information technology, cf. Fig. 1. Perceived usefulness essentially describes the degree to which a person believes that an innovation will boost their performance (Davis, 1989). Perceived ease of use on the other hand describes the degree to which a person believes that adopting an innovation will be free of effort. In effect, users are more likely to adopt systems, which are easier to use and offer some benefits, since these two factors can affect the behavioural intention to consider using it and actually using the innovation. Behavioural intentions are formed on the basis of an individual's attitude, subjective norms, and perceived control of an outcome [14].

Perceived usefulness, perceived ease of use and behavioural intentions will have already been proven to be a reliable means for determining adoption of technology [4], [15]. This study introduces aspects of trust and privacy in the design of privacy-enhancing IDMS. This is based on the premise that users will feel comfortable with systems that protect their privacy and are more likely to release personal information to only trusted third parties – the essence of user centricity [16].

III. FRAMEWORKS AND INITIATIVES

A. Regulatory Framework on Privacy

Motivations for good behaviour can generally be analysed based on the risk of data disclosure and regulatory exposure. Regulation in this regard can be categorized into national and international. The Fair Information Practice principles (FIP) are a set of such principles developed in the 1970s, which has been adopted by many government agencies, public interest groups, and private companies around the world [5]. The Organization for Economic Cooperation and Development (OECD) issued a set of data protection guidelines, which are an adaptation of FIPs. These guidelines focus on privacy as personal data flows between member countries. It addresses the collection and use of personal data, such as names, addresses, government-issued identifiers, etc.

The OECD guidelines are very instructive for design of privacy-enhancing IDMS. The key sections are as follows [17]:

- *Collection limitation.* Limits to the collection of personal data should exist. Personal data should be collected by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject (the individual).
- *Data quality.* Personal data should be relevant to the purposes for which it is collected and used. It should be accurate, complete, and timely.
- *Purpose Specification Principle.* The purpose for which personal data are collected must be specified no later than at the time of date collection and subsequent use must be limited to the fulfilment of those purposes or such others as are not incompatible with the original purpose and as are specified on each occasion of change of purpose.
- *Use limitation.* Personal information should not be disclosed or otherwise used for other than a specified purpose without consent of the individual or legal authority.
- *Security.* Reasonable security safeguards against such risks as loss, unauthorized access, destruction, use, modification and disclosure should protect personal data.
- *Openness.* The existence of systems containing personal data should be publicly known, along with a description of the system's main purposes and uses of the personal data in the system.
- *Individual Participation.* An individual should have the right: a) to obtain confirmation from a data controller, or otherwise, any information relating to them within a reasonable time. The cost of obtaining such information must be reasonable and in a form that is readily intelligible to him.
- *Accountability.* The keepers of personal data should be accountable for complying with fair information practices. These principles are the logical starting point for anyone designing an identity management system.

There are also various country- (or region-) specific laws on privacy that seek to protect privacy. In Europe for instance, many of the privacy and data protection laws have been brought together as a harmonized European Union (EU) data protection directive. All EU member states are required to comply. The Directive provides mechanisms to track misuse of personal data and protection against the mis-

application of personal data [18]. Unlike the FIPs, bleaching legislations and directives can result in prosecution in courts.

The major defects of the regulatory framework are two-fold. In the first place, FIPs originate long before the World Wide Web and the digital age [5]. Hence, they are inadequate in dealing with modern privacy since acquisition and use of personal information occurs in microseconds and usually with no direct involvement of parties. Secondly, on the Internet, there are no specific border demarcations, making it difficult to enforce country- or region-specific laws on privacy and data protection. This is because culprits might not be nationals of the countries, where the incidence occurred (e.g. the WikiLeaks cases).

B. User-Centric Identity Management Systems

The focus on users' quest for power to exercise informational self-determination has resulted in several user-centric and claims-based IDMS initiatives (PrimeLife, 2009), (FIDIS, 2007), (Cameron, 2005). User-centric IDMS is an approach to give users greater control over their personal information. However, the notion of user centricity does not imply a trade-off between security and usability, but rather a focus on user's privacy and trust. For instance, in their Austrian IDMS study, Aichholzer & Strauß (2009) identified equality of access, privacy protection and user convenience as major factors determining users' acceptance of IDMS. Cameron's Seven Laws of Identity have therefore been widely regarded as a guide for providing user-centric IDMS solutions. Generally, the laws of identity prescribe the need for consistent user experiences in online transactions, user understanding, user choices and control, and minimum disclosure of user information to only the intended parties.

Identity providers therefore act as trusted third parties to store user accounts and profile information and authenticate users [19]. Service providers on the other hand accept assertions or claims about users from the identity providers. Since identity providers do not form a federation in a user-centric IDMS model they are seen as operating in the interest of users instead of the service providers (also called "relying parties").

A feature in user-centric IDMS, which makes them more privacy enhancing, is the fact that users have the privilege of choosing what information to disclose when dealing with service providers in particular transactions and still satisfy the need to provide certain information for the transaction require [19], [20].

C. Privacy Research Initiatives

To address the inefficiencies of regulations discussed above, a wide range of industry, academic, and governmental organizations in Europe joined forces in a number of research projects, among these "*Privacy and Identity Management for Europe (Prime)",* and *"Privacy and Identity Management in Europe Throughout Life (PrimeLife)"* [21]. These projects have developed working prototypes of privacy-enhancing IDMS, These EU initiatives provide very good frameworks for building privacy-protecting IDMS, although they do not cover US specific regulations.

Kim Cameron, Microsoft Identity Architect, and Ann Cavoukian, Ontario's Information Privacy Commissioner, have done a lot of research on privacy, which is becoming industry standard. In her paper, "7 Laws of Identity: The Case for Privacy-Embedded Laws in the Digital Age," Cavoukian (2008) offered a unique interpretation of Cameron's Laws of Identity. Cavoukian further proposed seven foundational privacy principles, referred to as Privacy by Design (PbD) principles. Her proposal was based on the notion that innovation, creativity and competitiveness must be approached from a design thinking perspective [22]. In a separate study, Peter Schaar posits that "PbD is adjuvant for all kinds of IT systems designated or used for the processing of personal data. It should be a crucial requirement for products and services provided to third parties and individual customers." [3]. Table I provides a summary of the seven laws of identity, the FIPs and Cavaokian's PbD.

TABLE I
MAPPING OF THE LAWS OF IDENTITY, PRIVACY BY DESIGN AND THE FAIR INFORMATION PRACTICES

Seven Laws of Identity	**FAIR INFORMATION PRACTICES (FIP)**	**Privacy by Design**
1 – User Control and Consent: Technical identity systems must only reveal information identifying a user with the user's consent	Collection limitation	Privacy as the default setting
2 – Minimal Disclosure for a Constrained Use: The identity metasystem must disclose the least identifying information possible, as this is the most stable, long-term solution.	Data quality	Privacy as the Default Setting
3 – Justifiable Parties: IDMSs must be designed so the disclosure of identifying information is limited to parties having a necessary and justifiable place in a given identity relationship.	Purpose Specification Use limitation.	Privacy as the default setting
4 – Directed Identity: A universal identity meta system must support both "omnidirectional" identifiers for use by public entities and "unidirectional" identifiers for use by private entities, thus facilitating discovery and prevent unnecessary release of correlation handles	Security	End-to-End Security Full lifecycle protection Proactive and Preventive
5 – Pluralism of Operators and Technologies: A universal identity solution must utilize and enable the interoperation of multiple identity technologies run by multiple identity providers.	Openness	Visibility and Transparency –keep it open
6 - Human Integration: The identity metasystem must define the human user to be a component of the distributed system, integrated through unambiguous human-machine communication mechanisms offering protection against identity attacks	Individual Participation	Privacy Enhancing Design Full Functionality
7 – Consistent Experience across Contexts: The unifying identity metasystem must guarantee its users a simple, consistent experience while enabling separation of contexts through multiple operators and technologies	Accountability and Audit	Visibility and Transparency – Keep it open.

The seven laws of identity also describe the basis for a "unifying identity metasystem" that can be applied to identity on the Internet. The Identity Metasystem is an interoperable architecture for digital identity, which assumes that users will have several digital identities based on multiple underlying technologies, implementations, and providers [1]. It ensures that not only are individuals in control of their identity, but also organizations will be able to continue to use their existing identity infrastructure investments, choose the identity technology that works best for them, and more easily migrate from old technologies to new technologies without sacrificing interoperability with others [1].

The major informational privacy [23] emanating from digital identities in the identity metasystem are observability and linkability. Observability is the possibility that others, including communicating parties, service providers, eavesdroppers and third parties will gain information. Linkability on the other hand describes the possibility of linking different data or data sets to an individual for further analysis.

IV. Privacy-Enhancing Technologies

The move to online services offers great promise in terms of both cost reduction and improved user experience. However, the realization of this promise has been severely hampered by the lack of trust on the Internet – specifically, the absence of a practical mechanism for users to obtain and present strong, verified digital identity information online. In some cases, the information simply is not available in a digital form; however, even when it is available, the current set of identity technologies force a trade-off between the level of identity information assurance that can be achieved and the level of privacy given to users. Further, the user's experience for providing this information is often inconsistent and difficult, and sometimes redundant.

Digital identity must embrace both being public and being private by providing both anonymity and pseudonymity. It always exists in a context, and we expect the context to have the same degree of separation, which we are used to in the natural world, even though space and time no longer serve as insulation.

In a user-centric IDMS, the issue of distrust between the user and the relying party is addressed, because the identity provider acts as a trusted third-party broker. This occurs because individuals may have several identity providers and for that matter, their information may not be stored in one place. User will naturally trust brokers they can control whereas relying parties will not trust a broker if the claims asserted are actually self-vouched by the user [16], [19].

This is what the U-prove and OAuth technologies seek to address by managing claims and attributes so that relying parties are assured that the information is correct before engaging with the user, without necessarily revealing the identity of the user. This approach will still leave the user in control. U-Prove and OAuth enable the use of services with minimum disclosure of personal information and fine-grained delegation of authorization between service providers. Some of their features are summarized in the following.

A. U-Prove

U-Prove is an advanced cryptographic software designed for electronic transactions and communications to overcome a long-standing dilemma between identity assurance and privacy already mentioned [19], [24]. The technology is part of Microsoft's drive to promote an open identity and access model for individuals, businesses and governments, based upon the principles of the identity metasystem [1].

The dilemma is addressed by enabling minimal disclosure of identity information in electronic transactions and communications. To ensure minimum disclosure the U-Prove Agent software acts as an intermediary between websites. This allows users to share data in a manner that protect their privacy, since they can now choose to share or otherwise. U-Prove includes a mechanism that separates the retrieval of information from trusted third parties from the release of this information to the destination site. This implies that the organization issuing the information is prevented from tracking where or when information is used. The destination site is similarly prevented from linking users to their activities.

B. OAuth

Open Authorisation (OAuth) is an open standard for authorization, which gives users the ability to grant third-party access to their resources without sharing their passwords [25]. It also provides a way to grant limited access (in scope, duration, etc.). OAuth allows users to share their private resources (e.g. photos, videos, contact lists, bank accounts) stored on one site with another site without having to hand out their credentials, typically username and password. The concept of OAuth is based on the metaphor of a valet key of car, since it only gives third parties a controlled (limited) access to the car [26], [25]. OAuth mimics the valet key metaphor by providing sites with just enough information to accomplish what the user has requested, but not allowing third-party sites access to any other user information. Precisely, it only allow users to hand out to third parties tokens (instead of credentials) to their data hosted by a given ser-

TABLE II
Analysis of U-PROVE and OAUTH in the Light of the User-Centric Solutions

DESCRIPTION	U-PROVE	OAUTH
Purpose of the Application	Designed for Electronic Transactions and Communication	For information sharing on the internet
Coverage		Video, Photos and Contact List
Minimal Disclosure		
Trust	Uses Cryptography	Does not use Cryptography
User Control & Consent	Does not allow profiling	Users can grant 3rd access personal resources without sharing password
Privacy		
Perceived Trust		
Pluralism of Operators and Technologies		OAuth works on Desktop Applications Mobile Phones and Living room devices
Privacy as Default	Uses Advanced Cryptography	
Perceived Usefulness	Has both Open Standard and Application specific versions	Uses Open Standard
Human Integration	Permit local storage of U-prove tokens	OAuth 2 is Client Developer Centric. Users can easily develop applications on OAuth platform
Perceived Ease of Use		

vice provider. The tokens could be granting a printing service access to photos without sharing username and password. OAuth 2.0, which is the latest version, focuses on client developer simplicity (not user simplicity) while providing specific authorization flows for web and desktop applications, mobile phones, and living room devices [25].

Table II presents some of the main features of U-Prove and OAuth and compares them with the privacy design principles discussed above.

V. Improved Framework and Guidelines

The fact that present privacy laws are based on principles drafted many years ago, when the web did not exist, shows that privacy legislation need to make a quantum leap to be in line with the realities of today's real life operating environment. In cyberspace, there are no clear visual cues about the level of privacy available [7]. Existing privacy legislations and regulations do not adequately deal with digital identity issues, because laws are country- or region-specific, and the FIPs are not laws.

Important privacy considerations are in relation with data collection, data usage, storage, data minimization, anonymity, pseudonymity, and the extent to which individuals have control over how their personal information. Generally, identity systems that facilitate anonymity and pseudonymity may offer better promise of privacy. In essence, to ensure privacy, risk of vulnerability, the lifespan of identity information, and the costs of processing, storage and deletion are critical.

Linking identities that do not share the same degree of anonymity, or that contain different sets of attributes may allow others to overcome pseudonyms and discover the user's identity. Differences may arise as to which practices of identity and other data collection, use, and retention can be left to market forces and those that should be the subject of government intervention. Controlling linkability involves both maintaining separate contexts so observers cannot accumulate sensitive data and being cautious when identity information is requested to keep track of information disclosure [5].

Since much of the literature on privacy enhancing initiatives aims at introducing technologies with the user in mind it was apparent that the analysis is carried out in the light of Technology Acceptance Model. For instance if privacy must be at the core of the design [22], then obviously the original TAM must be extended to include privacy as a construct. Likewise, to address the dilemma between identity assurance and privacy, trust must also be added as a construct.

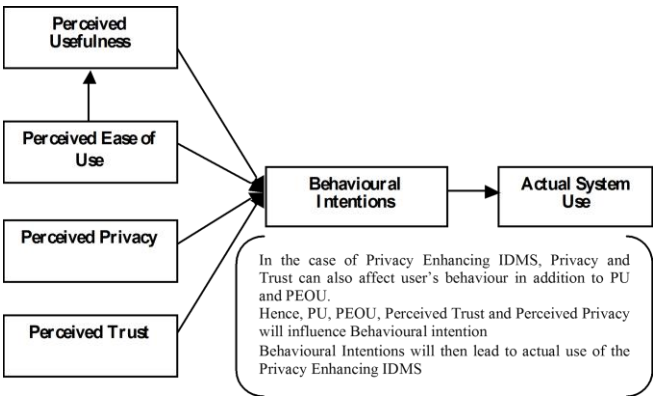

Fig.2. Technology Acceptance Model applied to privacy-enhancing identity management. The diagram shows that users' privacy behaviour is influenced by how easy it is to use the IDMS, and their perceptions on the system's usefulness, privacy and trust considerations. This behaviour then influences the actual system use. *(Adapted from* [4]*).*

We therefore propose to add Perceived Privacy and Perceived Trust as constructs to the original TAM, cf. Fig. 2. As shown in the diagram Perceived Usefulness, Perceived Ease of Use, Perceived Trust and Perceived Privacy will affect users' behavioural intentions and in the end their decision to conveniently use the IDMS.

IDMS having privacy design flaws can generate adverse consequences for consumers, including the risk of identity theft. On the contrary, IDMS can play a privacy protective role, particularly in the context of social interactions.

TABLE III
Factors to be Considered in the Design of Privacy-Enhancing IDMS

Item	Measurement Criteria	Description
Perceived Usefulness	Ease of Use Enhanced Security Identity Fraud prevention Data Quality	Perceived usefulness describes the degree to which a person believes that an innovation will boost their performance
Perceived Ease of Use	User-Centricity Universal Coverage (Online/Offline)	Perceived ease of use describes the degree to which a person believes that adopting an innovation will be free of effort.
Perceived Privacy	Best Practices Regulations, Privacy by design	Application of Laws, Regulations and the laws of identity (see table 2)
Perceived Trust	Ability	The group of skills, competences and characteristics that enable a person to have some influence within a domain or context (Mayer, Davis, & Schoorman, 1995)
	Benevolence	The extent to which the trustee is believed to want to do good to the *trustor* irrespective of profit motives.
	Integrity	Integrity is the perception that the *trustee* will adhere to a set of principles that the *trustor* subscribes to.

On the basis of this extended theoretical framework recommendations for improved design of privacy-enhancing IDMS can be derived. Table III is a summary of the major items, which must be taken into consideration during the design of privacy-enhancing technologies. For instance, the concept of privacy will result in a system having privacy as a default [22]. Similarly, trust considerations will help in overcoming the "dilemma between identity assurance and privacy [19], [24].

VI. Findings & Conclusion

This study analysed the concepts of privacy, trust, and the key regulatory and research initiatives on privacy enhancing IDMS. Major frameworks including the Laws of Identity, the Fair Information Practices principles and the Privacy by Design principles were examined. As a result, we found that perceived privacy and perceived trust should be added as constructs to the Technology Acceptance Model, in order to adequately represent privacy-enhancing identity manage-

ment for the benefit of users and service providers. This also aids in resolving the “Privacy Paradox” and resolving the dilemma between privacy and identity assurance.

The extensive amount of research in this area has lead us to the stage, where we now have a fairly good understanding of design principles and best practices, and we also start to have technologies available for development of services and solutions that can empower users, protect their privacy and support fine-grained control of access to resources online. This work is therefore an important contribution to the further development.

One of the remaining issues is to explore how these frameworks and technologies can address privacy and identity management in the physical world. The mechanisms of establishing trust in the physical world are not necessarily the same as those that are used in the digital world online. As it has been phrased “the Internet was built without a way to know who or what you are connecting to” [1]. Many of the recent initiatives are aimed at establishing an “identity layer” on the Internet. But since physical identity cards, tokens etc. are use in both worlds we need more work to link the usage and achieve “human integration” [1]. Users need to feel equally comfortable consuming services in the physical and digital world.

REFERENCES

[1] K Cameron. (2005) identityblog [Online] http://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf.

[2] Ann Cavoukian, "The case for privacy-embedded laws of identity in the digital age. ," 2008.

[3] Peter Schaar, "Privacy by Design," *Springerlink*, April 2010.

[4] 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.

[5] Marit Hansen, Ari Schwartz, and Alissa Cooper, "Privacy and Identity Management," *IEEE Security & Privacy*, 2008.

[6] Raffaele Zallone, "The Privacy Paradox or How I Learned to Have Rights that Never Quite Seem to Work," in *AAAI Spring Symposium Series*, Palo Alto, California, 2010.

[8] David Mason and Charles D Raab, "Privacy, Surveillance, Trust and Regulation: Individual and Collective Dilemmas of Online Privacy Protection," *Information, Communication & Society*, vol. 5, no. 3, p. 379 — 381, 2002.

[7] Priscilla M. Regan, "Privacy as a Common Good in the Digital World, ," *Information, Communication & Society*, vol. 5, no. 3, pp. 382-405, 2002.

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

[10] Robert M Morgan and Shelby D Hunt, "The Commitment-Trust Theory of Relationship Marketing," *The Journal of Marketing*, vol. 58, no. 3, pp. 20-38, July 1994.

[11] Audun Jøsang, John Fabre, Brian Hay, James Dalziel, and Simon Pope, "Trust requirements in identity management," in *Australasian workshop on Grid computing and e-research*, vol. 44, 2005.

[12] Patricia A. Norberg, Daniel R. Horne, and David A. Horne, "The Privacy Paradox: Personal Information DisclosureIntentions versus Behaviors," *The Journal of Consumer Affairs*, vol. 41, no. 1, 2007.

[13] Dennis Calton, Peter Graham, and John Reiners, "Resolving the "privacy paradox" Practical Strategies for Government Identity Management Programs," 2008.

[14] Icek Ajzen, "From Intentions to Actions: A Theory of Planned Behavior," in *Action Control: From Cognition to Behavior*. New York: Springer-Verlag, 1985.

[15] S Dass and S Pal, "Feasibility and Sustainability Model for Identity Management," India, 2009.

[16] Audun Jøsang and Simon Pope, "User Centric Identity Management," in *AusCERT Conference*, 2005.

[18] Michael D. Birnhack, "The EU Data Protection Directive: An engine of a global regime," *Computer Law & Security Report*, vol. 20, pp. 508–520, 2008.

[17] OECD. OECD Guidelines on the Prrotection of Privacy and Transborder Flows of Personal Data. [Online]. http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html

[19] OECD, *The Role of Digital Identity Management in the Internet Economy: A Primer for Policy Makers*, OECD Digital Economy Papers ed.: OECD Publishing, 2009, vol. 160.

[20] Georg Aichholzer and Stefan Strauß, "The Citizens Role in National Electronic identity Management: A Case-study of Austria," in *Second international Conference on Advances in Human-Oriented and Personalized Mechanisms, Technologies, and Services*, Porto, Portugal, 2009.

[21] PrimeLife, "From H1.3.5: Requirements and concepts for identity management throughout life," 2009.

[22] Ann Cavaokian. (2010, May) Information and Privacy Commision, Ontario. [Online]. http://www.ipc.on.ca/images/Resources/pbd-implement-7found-principles.pdf

[23] Alan F. Westin, "Social and Political Dimensions of Privacy," *Journal of Social Issues*, vol. 59, no. 2, pp. 431-453, 2003.

[24] Microsoft_Connect. (2010, Mar) Microsoft Connect. [Online]. https://connect.microsoft.com/site1188

[25] Eran Hammer-Lahav. (2007, Oct.) hueniverse. [Online]. http://hueniverse.com/2007/10/beginners-guide-to-oauth-part-i-overview/

[26] P.J Connolly, "OAuth is the 'hottest thing' in identity management," *eWeek*, vol. 27, no. 9, pp. 12-13, May 2010.

[27] Faye Fangfei Wang and Nathan Griffiths, "Protecting privacy in automated transaction systems: A legal and technological perspective in the European Union,"

International Review of Law, Computers & Technology, vol. 24, no. 2, pp. 153-162, 2010.

[28] George R Milne and Maria-Eugenia Boza, "Trust and Concern in Consumers' Perceptions of Marketing Information Management Practices," *Journal of Interactive Marketing*, vol. 13, pp. 5–24., 1999.