The Limits of Control – (Governmental) Identity Management from a Privacy Perspective

Stefan Strauß[1]

[1] Institute of Technology Assessment, Austrian Academy of Sciences, Strohgasse 45/5, 1030 Vienna, Austria
sstrauss@oeaw.ac.at

Abstract. The emergence of identity management indicates that the process of identification has reached a stage where analog and digital environments converge. This is also reflected in the increased efforts of governments to introduce electronic ID systems, aiming at security improvements of public services and unifying identification procedures to contribute to administrative efficiency. Though privacy is an obvious core issue, its role is rather implicit compared to security. Based on this premise, this paper discusses a control dilemma: the general aim of identity management to compensate for a loss of control over personal data to fight increasing security and privacy threats could ironically induce a further loss of control. Potential countermeasures demand user-controlled anonymity and pseudonymity as integral system components and imply further concepts which are in their early beginnings, e.g., limiting durability of personal data and transparency enhancements with regard to freedom of information to foster user control.

Keywords: privacy, IDM, e-ID, user control, e-government, transparency, freedom of information

1 Introduction

The role of identity is changing in the information society as every day life becomes increasingly pervaded by information and communication technologies. Novel and more sophisticated online services are emerging and transaction services are becoming mainstream activities [1]. Together with a significant increase in personalization, a growth in the provision and processing of personal data is inevitable. This development reinforces concerns about security and induces a certain demand to facilitate individuals in controlling their personal data and safeguarding their privacy. Identity management (IDM) deals with this demand and has become an emerging field of research in the information society [2]. E-government was one important trigger for the introduction of systems for electronic identity management (e-IDMS). Functional equivalents to traditional forms of identification in service relationships have to be developed for a digital environment. Thus, many governments in Europe and world-wide have already introduced e-IDMS or are about to do so. Most of the current systems are based on smart card technology as it allows

to combine possession (i.e., the card) and knowledge (i.e., a PIN) and thus provides a higher level of security than knowledge-based concepts (i.e., username and password) without a physical device. The carrier device for the electronic ID (e-ID) is not necessarily a chip card; there are also other tokens possible (e.g., mobile phones or USB-devices). But as chip cards already enjoy a broad range of use (e.g., ATM cards, social security cards), these are the preferred tokens [3; 4; 5].

The e-ID usually fulfills two functions: the unique identification of a person and the authenticity of her request. The primary intent is to enable and strengthen secure and trustworthy interactions between government, citizens and businesses. Further intentions aim at improving security of e-commerce and at enabling new business models. Governments expect higher levels of security, efficiency and cost-effectiveness of electronic communication and transactions to be major benefits of a national e-IDMS, for the public administration itself as well as for citizens and businesses. The two central objectives of this trend towards national e-IDMS are: to improve security of online public services and to unify identification and authentication procedures of these services.

Identification is a core function of governments and thus the creation of national e-ID systems implies far reaching transformations with many different aspects involved (e.g., technological, organizational, legal, political) [6], which contribute "to alter the nature of citizenship itself" [7]. Thus, e-ID is more than a device for citizen identification; it becomes a policy instrument. Following the distinction between "detecting" and "effecting" tools of government [8], the e-ID more and more shifts from being a "detecting" tool to an "effecting" tool. While the former primarily addresses an instrument for supporting administrative procedures such as the ascertainment of identity in public services, the latter terms an instrument for governments to enable services and to impact societal and political objectives [3]. This is inter alia reflected in information society policies of the European Union: an e-IDMS is seen as a "key enabler" for e-government [9]. The vision is to set up a "pan-European infrastructure for IDM in support of a wide range of e-government services" [4]. Introducing national e-ID (and in a long term view also of an interoperable e-IDMS for Europe) is also seen as instrument to fight identity fraud and terrorism [4]. According to the EU action plan i2010, "one safeguard against identity fraud" is the "[a]ssertion of the authenticity of online identity" and the "easier ownership and management of personal/business data" [9].

Privacy is obviously of vast importance for e-ID. However, current governmental e-IDMS developments seem to explicitly focus at improving administrative efficiency and security, while privacy seems to be a rather implicit objective. The sometimes tense relations between privacy and security[1] are also visible in the e-ID discourse (cf. [6], [7]). The capability of an e-IDMS to enhance privacy naturally depends on the concrete system implementation and its surrounding framework it is embedded in.

This paper aims to contribute to make the treatment of privacy in (governmental) IDM more explicit in the e-ID discourse and to reveal potential impacts in this regard. Of special interest are the limits of IDM regarding user control and self-determined

[1] Security in the e-ID context primarily means information security not national security although there are many intersections between both. However, a detailed incorporation of national security aspects would exceed the scope of this paper. For an in-depth analysis of identity cards with a focus on national security issues see e.g., [3] [7] [[24].

handling of personal data and relevant aspects for overcoming these limits. The analysis includes major privacy aspects of IDM, their implementation in national e-IDMS as well as an assumed control dilemma of IDM. Based on these issues, potential threats to individual privacy and emerging challenges will be discussed. To some extent the paper ties in with results of a previous comparative research project (conducted in 2008/9) about selected national e-IDMS [10]. The author was involved in analyzing the innovation process of the Austrian system, where a combination of different methods were applied: 20 interviews with major e-government stakeholders, complemented by a literature review, an analysis of official documents, discussion statements, technical specifications, and practical tests in a user role. The paper is structured as follows: Section 2 describes IDM in a privacy context and outlines preconditions for privacy-enhancing IDM; Section 3 deals with their implementation in governmental e-IDMS. In Section 4 the control dilemma of e-IDM and its major determinants are explained. Section 5 discusses how to resolve this dilemma and Section 6 concludes with the major findings of the paper.

2 IDM and concepts for privacy protection

A general definition describes IDM as "the representation, collection, storage and use of identity information" [11]. Of vast importance for IDM is the (often neglected) fact, that every individual is not represented by one universal identity, but has multiple identities in different contexts. There is no such thing as 'the identity' [12] and hence IDM can be more specifically described as "managing various partial identities (...) of an individual person (...) including the development and choice of the partial identity and pseudonym to be (re-)used in a specific context or role" [12]. Privacy-enhancing IDM combines privacy and authenticity [13]. Obviously, central privacy principles (such as commensurability, purpose limitation, data minimization, transparency) have to be fulfilled to allow for informational self-determination [14] [1].

2.1 User control

User-centricity and the users' control over their personal data respectively their identities are essential aspects for privacy protection. The e-ID should facilitate users in controlling which data they want to share and in which different contexts these data are allowed to be processed and linked. In cases where this is not feasible users should at least be able to comprehend who processed their data, on what foundation and for which purpose [13; 14] [1]. Managing different (partial) identities is important for purpose limitation, where only data absolutely required for a specific context should be processed. In this regard, the concepts of anonymity and pseudonymity are relevant. In conjunction with governmental e-IDMS, one might presume that in every context which does not require identification or even demand for anonymity, the e-ID should not be used at all. However, due to tendencies towards ubiquitous computing which imply a significant decrease of areas of anonymity [15], this might be insufficient. Particularly, when considering that an "identity as a set of attribute

values valid at a particular time can stay the same or grow, but never shrink" [16]. Hence, it seems expedient to incorporate anonymity as an integral element into the system.

2.2 Unlinkability

The linkage of personal data for profiling beyond the individual's control is a particular menace to privacy, which primarily derives from the use of unique identifiers. Thus, unlinkability is one crucial property that must be ensured to prevent "privacy-destroying linkage and aggregation of identity information across data contexts" [1]. The efficient implementation of unlinkability is a sine qua non of privacy-enhancing IDM [17]. A precondition is the use of pseudonyms in different contexts according to the intended degree of (un)linkability. In [12], five forms of pseudonyms are described: transaction pseudonyms enable the highest level of unlinkability and thus strong anonymity. Each transaction uses a new pseudonym, which is only applied for a specific context[2]. A person pseudonym, i.e., a substitute for the civil identity of the holder (e.g., a unique number of an ID card, phone number or nickname) provides the lowest anonymity level. Moderate linkability is given by role and relationship pseudonyms, which are either limited to specific roles (e.g., client) or differ for each communication partner.

Closely connected to unlinkability is the significance of decentralized data storage as well as context separation. Hence, personal data should be separated in as many different domains as possible to prevent data linkage [1]. For data minimization only data that are absolutely inevitable should be processed (e.g., age verification does not demand knowing the date of birth. A query whether the date is over or under the required date is sufficient).

3 Privacy incorporation of governmental e-IDMS

Several different dimensions including technical, organizational, legal and socio-cultural aspects influence a system's particular shape. This is one explanation for European e-IDMS having several differences regarding technical design and privacy features [5], whereas the latter are "by no means universally implemented" [18]. Although privacy-enhanced techniques for public key infrastructure (PKI) have already existed for several years, these techniques have scarcely been adopted in mainstream applications and e-ID card schemes [18]. Hence, the level of unlinkability is rather diverse. Exceptions are e-IDMS in Austria and Germany, which "have taken some important steps towards unlinkability and selective disclosure" [18]. Most European systems utilize unique identifiers which are often derived from national registers (e.g., social security, public registration). Some store these identifiers directly on the device (e.g., Belgium), others in an encrypted form. In Austria the unique identifier from the Central Register of Residents (CRR-no.) is used, which is unique for every citizen. The device only contains an encrypted version of the CRR-

[2] E.g., transaction authentication number (TAN) method for online banking.

no., the so-called sourcePIN. For identification during services, this sourcePIN is not used directly either. Instead, sector-specific identifiers (ssPINs) based on an irreversible cryptographic function are created, which are unique for 26 sectors; one ssPIN allows unique identification only in the corresponding sector. Such sectors are for instance tax, health and education. To prevent privacy abuse, storing an ssPIN is restricted to the sector it belongs to or that is allowed to use it [10]. The sophisticated concept is similar to a relationship pseudonym as a person is always identified with the same ssPIN in a specific sector. Although this approach theoretically allows users to manage partial identities, pseudonymity is not sufficiently implemented yet and serious privacy concerns remain. The ssPINs are used to avoid linkability and are unique for each person. However, one of the 26 sectors is delivery (of verdicts, official documents etc.) which is part of almost every public service. As every authority providing a service that includes delivery is able to process the corresponding ssPIN, critics suspect that privacy infringement is feasible as a person's data is linkable with this PIN over different contexts [10]. As identity data (e.g., name, address, date of birth) are still being processed in almost every service, the use of ssPINs does not sufficiently protect from illegal data linkage [10] [19]. Processing these data might be necessary for e-government transactions, but not per se for every service (e.g., information services). Currently, the user has neither influence over the pseudonyms used, nor over which of her data is processed in an application. Thus, users have very limited control over their e-ID.

4 The control dilemma of e-ID

Current e-IDMS are lacking in privacy enhancement, especially as unlinkability is mostly as yet insufficiently provided. This circumstance, combined with the main objectives of IDM can be described as a control dilemma: IDM primarily aims to improve security of e-transactions and unify authentication with privacy as an implicit aim. Or, more generally: the increasing relevance of IDM can be seen as a demand to regain control over personal data flowing in digital environments. On the other hand, tendencies towards e-ID and personalization may lead to further services which require identification. This would imply a significant reduction in anonymity. In other words: the attempt to compensate for a loss of control would ironically, at least from a user's point of view, induce yet a further loss of control over personal data. The following subsections highlight some critical aspects to explain the dilemma.

4.1 "Identity shadow" - data linkage without unique identifiers

Due to poor pseudonym management, current e-ID card schemes are often provided with more information than necessary and thus allow "unnecessary disclosure of personal data via linkage between different transactions" [18]. A basic precondition for unlinkability is that utilization of a pseudonym does not entail further information which allow for data linkage. However, as e-ID usage usually entails further data, these can undermine unlinkability. I subsume these under the term „identity

shadow“[3]. This term comprises all the data appearing in a digital environment which can be used to (re-)identify an individual beyond her control and/or infringe her privacy.

One possibility for data linkage is given by utilizing semi-identifying data or quasi-identifiers, which are not necessarily unique but are related to a person [19; 20]. In almost every (e-government) service, a set of common data (CD) is requested or is a byproduct. The common data can be e.g., distinguished in a) person-specific data, which usually has to be entered in web-forms during a user-session (typical examples are name, date of birth, postal address, e-mail address, ZIP code); b) technology-specific data, which refer to the technical devices involved in the e-ID session (e.g., the number of the smart card, MAC-address, IP-address). This data can be used to gather quasi-identifiers which enable cross-linkage of separated data without the need of a unique ID. Thus, using sector-specific identifiers alone is not sufficient to prevent privacy infringement. Hence, the e-ID itself could become a privacy threat.

The size of the identity shadow depends on the amount of data the e-ID entails. E.g., a mobile phone as e-ID device might provide more data than a chip card, such as the mobile phone number, geo-location, the IMEI of the SIM card. Data traces of online activities (e.g., meta data, web browser history) offer further entry points for de-anonymization: e.g., data of web browsers can be exploited to (re-)create a digital “fingerprint” for uniquely identifying a specific user [21]. Social networks offer further ways to gather quasi-identifiers, as demonstrated in [22]. Individual users were de-anonymized by applying the web browser history attack and exploiting information of users' group memberships (social networks have only limited impact on governmental IDM yet. However, further e-ID-diffusion could change this). Further potential threats may arise from protocol data which occur during the creation of elements required for e-ID. Although the function of log files is to detect unauthorized access and protect e-ID abuse, it can also be used for privacy breaches: if every creation and usage of the e-ID items is stored in log files, then these files provide a rather comprehensive profile of the users’ activities in cyberspace. Hence, log files can be abused for profiling activities. Figure 1 shows the different aspects and the idea of the identity shadow:

[3] In recognition of the work of Alan Westin: Privacy and Freedom, 1967 and the term “Data Shadow“.

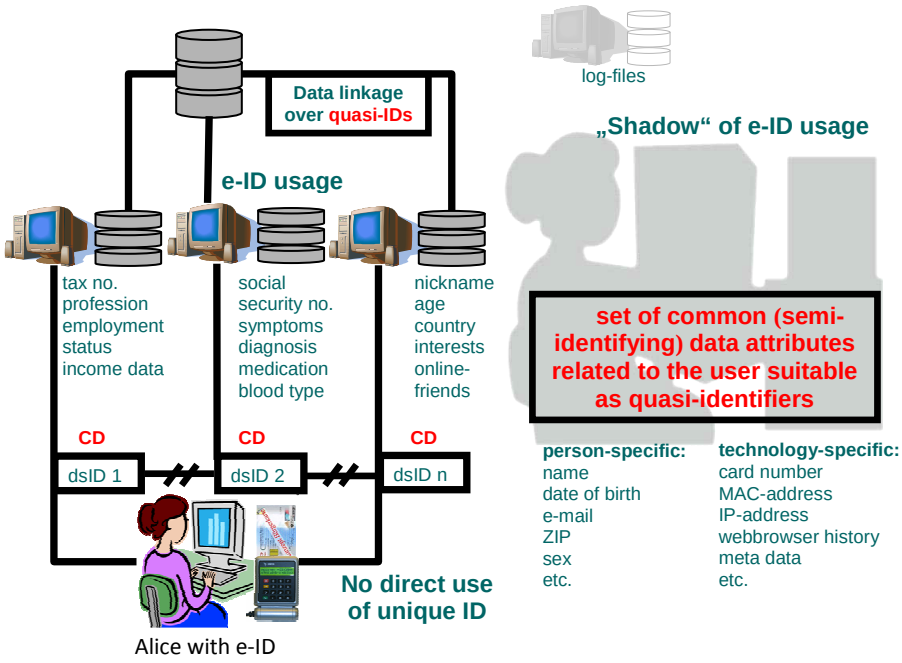

Fig.1. The identity shadow. Alice uses her e-ID for different services, e.g., for doing her tax declaration, for different health services or for a social network. The identity shadow describes the problem, that despite of the use of domain-specific identifiers (dsID) for providing unlinkability, data can still be linked over other common data (CD) which can be used to gather quasi-identifiers.

As the identity “never shrinks” [16] the identity shadow cannot be expected to do so either. Current and future trends (increase of browser-based applications, mobile services, cloud computing, RFID, biometrics, etc.) towards pervasive computing environments with a further growth of data traces will make this threat even more challenging.

4.2 Function creep

In our context, the danger of function creep addresses the extended use of identification data for purposes it was not originally intended for. One problem is an incremental obligation to identification, which seems plausible in an increasingly pervasive computing environment. Obligation is not just meant in the sense of legal compulsion for e-ID, where one could argue that the problem might be avoided by keeping e-ID voluntary. However, an increase of a broader range of e-ID services leads to a situation, where the e-ID becomes de facto mandatory [7]. The growth of services demanding identification could lead to a violation of privacy principles such as data avoidance and commensurability [23]. Further e-ID applying might be convenient to some extent for services which demand identification anyway. But in

services which essentially do not require identification, this would be of real concern (e.g., information or communication services). With increasing identification anonymity more and more shifts from the norm to the exception. As one objective of governmental e-ID development is also to support e-commerce and to enable further business applications it is conceivable that private businesses extend its usage from securing e-transactions to further contexts where identification is not legally required (e.g., as customer card or even for social networks).

There is already evidence for function creep regarding e-ID cards in different countries and contexts (such as described in [3]). Some examples are: usage of e-ID for public libraries, health services, access control, age verification, chat rooms, online report of child abuse, public transport, social networks and online games [3].

Identification and surveillance are strongly interrelated (e.g., [7] offers a detailed analysis), and there are many historical examples for the abuse of personal data for social discrimination and population control (cf. [3] [4] [24]). The process of identification implies the classification and categorization of personal data for rationalizing citizens' identities [24] [7], because to proof one's identity requires at least one unique piece of personal data (typically a unique identifier), that serves as identification criteria. One aim of e-IDMS development is to unify the processing of personal data in the back office within public administration to make service provision for citizens and businesses more efficient. While this is an important objective for the public good, it also holds the danger that the classification of personal data leads to social sorting, i.e., "the identification, classification and assessment of individuals for determining special treatment (…)" [24]. The consequence is discrimination of special citizen groups which become classified as suspicious (e.g., unemployed, welfare receivers, criminal suspects, persons with a police record, etc.). This sort of discrimination is of course already a problem without e-IDMS but it might intensify with e-ID when the classification mechanisms become accelerated and lead to automatic decisions which reflect and foster already existing stereotypes or other prejudicial typing [24] [7]. A recent example which could lead to social sorting provides the current discussion in Germany about the creation of an electronic alien card analog to the recently created personal e-ID. While the storage of a fingerprint on the e-ID for Germans is voluntary, this storage is planned to be compulsory on this alien e-ID card.[4]

For good reason, i.e., to relativize power, governmental sectors are separated in democratic societies. Lacking context-separation in e-IDMS would imply linkability of per se separated domains. With tendencies towards centralizing identity-related data which flow "through a small number of standardized infrastructure components" [1], the vulnerability e-IDMS increases, entailing further risks for privacy infringement as data storage, linkage, and profiling from commercial as well as governmental institutions are facilitated with a "pervasive IDM layer" [1].

The danger of function creep intensifies in the angle of recent political measures towards extended monitoring of online activity for preventing crime: e.g., European Data Retention Directive[5], internet content-filtering plans[6] (i.e., against child abuse

[4] http://www.heise.de/newsticker/meldung/Elektronische-Aufenthaltskarte-fuer-Nicht-EU-Buerger-in-der-Diskussion-1083049.html

[5] http://epic.org/privacy/intl/data_retention.html

and copyright offense), or the INDECT project aiming to merge several surveillance technologies (e.g., CCTV, data mining, automatic threat detection) into one intelligent information system[7].

5 Resolving the dilemma – towards transparency-enhancing IDM

The ways out of this dilemma require measures embracing different determinants of privacy to foster the effectiveness and controllability of privacy protection. A necessity for adapting privacy regulations to the changed requirements due to new technologies has been pointed out by privacy experts for many years. This necessity becomes very much visible also in the e-ID discourse. Thus, new regulatory approaches might be demanded to cope with the challenges of electronic identities. However, this alone might not be sufficient as „lawful collection and processing of personal data does not prevent per se unethical or unjust decisions based on them" [14]. Hence, a combination of different measures involving technology as well as policy aspects is required. One crucial point is how to compensate the imbalance regarding this control over personal data between citizens and governments, as citizens have very limited control yet. This requires an explicit focus on improving user control in combination with privacy-enhancing IDM. Hence, user-controlled linkability of personal data based on thorough data minimization [12] and purpose limitation. One crux is the implementation of anonymity and pseudonymity as integral system components. Only few e-IDMS use pseudonym approaches which provide a certain degree of unlinkability and contribute to improving the security of e-transactions. If at all applied, e-IDMS so far always pre-create pseudonyms giving users very limited control over their e-ID as there is no possibility to use the e-ID for self-determined creating and managing pseudonyms [10; 18]. Providing pseudonym management as an additional option would enhance informational self-determination as one could freely handle her pseudonyms respectively partial identities and decide whether to be identifiable or not (in any case without ID-obligation). The implementation of unlinkability has to range throughout the whole system, i.e., also the inner system logics and the databases involved. Wherever possible, anonymous credentials or transaction pseudonyms should be used. Otherwise, e.g., when unlinkability is lacking in the back office, then the e-IDMS does not provide effectual privacy protection for the individual and is rather cosmetic. This aspect seems underrepresented in governmental e-ID discourse, as the procedures within the system, i.e., how personal data is being processed are mostly opaque and unrevealed from a users' point of view.

Effective prevention of de-anonymization demands data minimization. As digital data can be copied in no time to an arbitrary number of repositories and per default do not expire, technical approaches to limit data permanence might enhance control over

[6] http://www.ispreview.co.uk/story/2009/10/16/uk-mps-propose-action-to-filter-internet-traffic-and-stop-illegal-p2p-cut-offs.html

[7] http://www.telegraph.co.uk/news/uknews/6210255/EU-funding-Orwellian-artificial-intelligence-plan-to-monitor-public-for-abnormal-behaviour.html
http://www.indect-project.eu/

its timely durability. One could then decide whether data should be permanently or temporarily available. An expiration date contributes to privacy as it "is an instance of purpose limitation" [25]. One recent example for a technical approach of this idea is "Vanish"[8], which combines cryptographic techniques with bit torrent technology to create self-destructing data [26]. Similar concepts contribute to privacy-enhancing IDM. However, these approaches are in the early stages of investigation and development, e.g., in [27], the vulnerability of Vanish is described as well as some measures demanded to improve its security. Hence, before a practicable use of these concepts, further research is needed by all means. But even if a more practicable technical approach would already exist, an expiration date is not feasible in many applications and thus its practicability remains limited. However, the idea of an expiration date has to be understood not simply as a technical concept which cannot be realized in a strict sense, but more as a policy concept, which could contribute to induce a paradigm shift from the current status quo of storing data without any limits to a more prudent handling of personal data and information. But still, an expiration date will not solve the problem of imbalanced control over information [25].

This imbalance is a key determinant of the control dilemma. The system needs to have mechanisms integrated that allow citizens and the public sphere, to control the proper and legal use of the data processed within the e-IDMS. Hence, there are also other measures required to enhance user control in addition to technical concepts for privacy enhancement. One aspect of vast importance is transparency. "Without transparency one cannot anticipate or take adequate action" [28]. Only when users can comprehend how their e-ID is being processed they can protect their privacy. Low transparency and incremental ID-obligation could cause a situation similar to a panopticon: individuals have to reveal their ID without knowledge about whether and for what purpose it is used - analog to the uncertain presence of the guard in the watchtower. Consequences would be self-censorship and limited individual freedom [25]. In this respect, freedom of information (FOI) plays a vital role. It addresses "the right to know" of the public regarding government actions [29], aims to improve their controllability and thus to compensate the "knowledge asymmetry between profilers and profiled" [28]. Although freedom of information mainly addresses a policy paradigm aiming at scrutinizing governmental policies and actions [23], fostering this paradigm might contribute to privacy enhancement as well. FOI and privacy are strongly interrelated and data protection laws also include FOI principles such as the right to access one's own personal data. For e-ID, freedom of information mainly implies options to enhance user control in this respect. [28] argues for a shift from privacy-enhancing tools (PET) to transparency-enhancing tools (TET) to limit the threats of autonomic profiling of citizens. The basic idea of TET is to give users the possibility for counter-profiling, i.e., to support users in understanding how the system processes their personal data and "which profiles may impact their life in which practical ways" [28]. While PETs aim to protect personal data, TETs aim to protect from invisible profiling [30]. One important aspect here is supporting users in their right to information and granting them access to their personal records including information about how they are used, for what purposes, by whom and on which legal term. Some e-ID applications already include access to personal records (e.g., some

[8] http://vanish.cs.washington.edu

Austrian e-ID services grant access to tax, health or public registration records). However, current e-IDMS do not seem to follow a systematic approach in terms of FOI and transparency enhancement. Services that allow users to view their personal records are currently rather the exception than the norm and the insights users get into the e-IDMS are limited (e.g., citizens could also receive information about the progress of administrative procedures they are involved, access to public registers etc.). The existing applications do not reveal further information about how personal data are used[9]. This is a crucial aspect for transparency enhancement, as the mentioned knowledge asymmetry can only be reduced if the system allows grasping deeper insights into "the activities of the data controller" [30]. E.g., by providing users not just access to their personal records, but also by revealing information about how these are treated and processed within the system, which user profiles are created by whom for which purpose.

Such approaches are important to improve the currently rather opaque situation of e-ID from a user perspective and contribute to raise the users' awareness and comprehension of how their data is treated in the system. However, fostering transparency on an individual level for the single user is only one aspect of the transparency enhancement. The controllability of an e-IDMS cannot be merely a matter of individual users, because they are not in the position to verify whether personal data is properly protected within the system (e.g., by a certain level of unlinkability). Thus, transparency is not just demanded on an individual level but has to be implemented on a systemic level as well. On the systemic level, approaches to improve transparency of the system mechanisms on a larger scale should be implemented. A scenario might be conceivable where groups or institutions, typically privacy organizations, are enabled to verify proper treatment of personal data in the e-IDMS (e.g., with applications and tools that allow them to make random samples in order to check if unlinkability is given in databases and registers).

However, transparency enhancement is not to be understood only as a technical approach because the privacy challenges to cope with are primarily societal ones which require adequate measures on at least these two different levels. While one level addresses the implementation of options of improving transparency for the individual interacting with the e-IDMS, another level addresses possibilities on a larger scale for the civil society and institutional actors to comprehend and examine the e-ID system, its architecture and how individual privacy is being protected as well as the purpose of an e-ID processing on what (legal) foundation. These aspects cannot be considered by technical means only but require a deeper understanding of the role of transparency for privacy protection by government actors and stakeholders involved in e-IDMS development.

6 Summary and Conclusions

Governmental e-IDs are at the core of the relationship between citizens and governments and thus entail several transformations beyond a technological

[9] One exception is the Belgian e-ID that provides information about which government agencies accessed a users' personal record.

dimension. They are not just devices for identification but also policy-instruments connected to societal and political objectives. While the primary aims are improving security of online public services and administrative efficiency, privacy is a rather implicit goal somewhere in between these objectives. This is inter alia visible in the often neglected incorporation of privacy features. Some systems already contribute to strengthen security and privacy in e-government to some extent, but with a main focus on security of e-transactions. Crucial aspects, i.e., anonymity and pseudonymity are – compared to unique identification – so far underrepresented and need to become integral system components with respect to a sustainable privacy-enhancing IDM. While this is not yet implemented, further emerging challenges intensify the need for effective privacy concepts. If IDM does not respond appropriately, this could lead to the outlined control dilemma: despite of aiming to (re)gain control over personal data, e-IDMS itself could foster further loss of control over individual privacy. Several issues shape this: insufficient prevention of linkability, increasing threats due to the identity shadow with data traces facilitating linkage and de-anonymization, the evident danger of function creep and further potential surface for privacy abuse entailed by centralized IDM infrastructures. To resolve this dilemma, governmental IDM should first and foremost foster more strict concepts for unlinkability with user-controlled pseudonymity. Additional approaches might be expedient e.g., an expiration date of personal data to pro-actively support data minimization and purpose limitation. The major challenge is to compensate the imbalanced control over personal information. This implies to give citizens and the public possibilities to effectively control their personal data and the proper processing of personal data within the e-IDMS. Solutions for enhancing transparency on an individual as well as on a systemic level are demanded in line with FOI paradigms, of course in strict accordance with privacy principles. This could also lever accountability of public authorities for legal processing of personal data and thus contribute to citizens' trust in government. Additional research is necessary to reveal further determinants of the dilemma and to design appropriate strategies to cope with the resulting challenges. In order to make the concept of transparency enhancement practicable, further analysis is demanded regarding its role for privacy protection and its different dimensions, especially on a systemic level. The effectiveness of transparency does not least depend on an appropriate combination of legal and technological aspects as well as on proper system design regarding usability.

References

1. Rundle, M., Blakley, B., Broberg, J., Nadalin, A., Olds, D., Ruddy, M., Guimarares, M. T. M., Trevithick, P.: At a crossroads: "Personhood" and digital identity in the information society, No. JT03241547, OECD (2008) http://www.oecd.org/dataoecd/31/6/40204773.doc
2. Halperin, R., Backhouse, J.: A roadmap for research on identity in the information society, Identity in the information society, 1(1), 71-87 (2008)
3. Bennett, C. J., Lyon, D.: Playing the identity card - surveillance, security and identification in global perspective. Routledge, London and New York (2008)
4. Comité Européen de Normalisation (CEN), CEN/ISSS Workshop eAuthentication - Towards an electronic ID for the European Citizen, a strategic vision, Brussels (2004)

http://www.vaestorekisterikeskus.fi/vrk/fineid/files.nsf/files/EE116CC13DFC98D0C225708C002BA544/$file/WS-eAuth_Vision_document+V017.pdf
5. Kubicek, H., Noack, T.: The path dependency of national electronic identities - A comparison of innovation processes in four European countries. In: Identity in the information society. Online first (2010) DOI: 10.1007/s12394-010-0050-2
6. Kubicek, H., Introduction: conceptual framework and research design for a comparative analysis of national eID Management Systems in selected European countries. In: Identity in the information society. Online first (2010) DOI: 10.1007/s12394-010-0052-0
7. Lyon, D.: Identifying citizens - ID cards as Surveillance. Polity Press, Cambridge (2009)
8. Hood, C. C. and Margetts, H. Z.: The Tools of Government in the Digital Age. Second Edition (Public Policy and Politics). Palgrave Mcmillan, Hampshire (2007)
9. EU Commission: i2010 eGovernment Action Plan: Accelerating eGovernment in Europe for the Benefit of All, No. SEC (2006) 511, Brussels (2006)
10. Aichholzer, G., Strauß, S., Electronic identity management in e-Government 2.0: Exploring a system innovation exemplified by Austria, Information Polity 15(1-2), 139-152 (2010)
11. Lips, M., Pang, C.: Identity Management in Information Age Government. Exploring Concepts, Definitions, Approaches and Solutions. Research Report, Victoria University of Wellington (2008) www.e.govt.nz/services/authentication/library/docs/idm-govt-08.pdf
12. Pfitzmann, A., Hansen, M.: Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology version 0.33. (2010) http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.33.pdf
13. Clauß, S., Pfitzmann, A., Hansen, M., Herreweghen, E. V.: Privacy-Enhancing Identity Management, No. issue 67, Institute for Prospective Technological Studies (IPTS) (2005)
14. De Hert, P.: Identity management of e-ID, privacy and security in Europe. A human rights view. In: Information Security Technical Report 13, 71--75 (2008)
15. Roßnagel, A.: Datenschutz im 21. Jahrhundert. In: Aus Politik und Zeitgeschichte Band 5-6 (Digitalisierung und Datenschutz), 9--15 (2006)
16. Pfitzmann, A. and Borcea-Pfitzmann, K.: Lifelong Privacy: Privacy and Identity Management for Life. In: Bezzi, M., Duquenoy, P., Fischer-Hübner, S., Hansen, M. and Zhang, G. (eds): Privacy and Identity Management for Life, 5th IFIP WG 9.2, 9.6/11.7, 11.4, 11.6/ PrimeLife, International Summer School, IFIP AICT 320: pp. 1-17 Springer, Heidelberg (2010)
17. FIDIS: Privacy modelling and identity. Deliverable-Report 13.6. Future of Identity in the Information Society. (2007) http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp13-del13.6_Privacy_modelling_and_identity.pdf
18. Naumann, I., Hobgen, G.: Privacy Features of European eID Card Specifications: European Network and Information Security Agency (ENISA) (2009) http://tinyurl.com/2unj3la
19. Priglinger, S.: Auswirkungen der EU-DL Richtlinie auf die E-Gov-Welt. In: Jahnel, D. (ed.) Jahrbuch Datenschutzrecht und E-Government. Neuer wissenschaftl. Verlag pp. 267-283 Graz (2008)
20. Sweeney, L.: k-anonymity: a model for protecting privacy, Int. Journal on Uncertainty, Fuzziness and Knowledge-based Systems 10(5), 557-570 (2002)
21. Eckersley, P.: How Unique Is Your Web Browser? Electronic Frontier Foundation (EFF) (2010) https://panopticlick.eff.org/browser-uniqueness.pdf
22. Wondracek, G., Holz, T., Kirda, E., Kruegel, C.: A Practical Attack to De-Anonymize Social Network Users. Technical report, iSecLab (2010) http://tinyurl.com/yccfqqd
23. Pounder, C. N. M.: Nine principles for assessing whether privacy is protected in a surveillance society, Identity in the information society (IDIS) 1 (1), 1--22 (2008)
24. Lyon, D. (ed.): Surveillance as social sorting - privacy, risk and digital discrimination. Routledge, London (2003)
25. Mayer-Schönberger, V.: Delete: The Virtue of Forgetting in the Digital Age. Princeton University Press, Princeton, New Jersey: (2009)

26. Geambasu, R., Kohno, T., Levy, A., Levy, H. M.: Vanish: Increasing Data Privacy with Self-Destructing Data. In: Proceedings of the USENIX Security Symposium, Montreal, Canada (2009) http://tinyurl.com/nmwfg9
27. Wolchok, S., Hofmann, O. S., Heninger, N., Felten, E. W., Halderman, J. A., Rossbach, C. J., Waters, B. and Witchel, E.: Defeating Vanish with Low-Cost Sybil Attacks Against Large DHTs. (2009) DOI: 10.1.1.161.6643 http://www.cse.umich.edu/~jhalderm/pub/papers/unvanish-ndss10-web.pdf
28. Hildebrandt, M.: Profiling and the rule of the law. Identity in the information society 1(1), 55-70 (2008)
29. Mendel, T.: Freedom of information – a comparative legal survey, 2nd edition. UNESCO, Paris (2008)
30. FIDIS: Behavioural Biometric Profiling and Transparency Enhancing Tools. Deliverable Report 7.12. Future of Identity in the Information Society (2009). http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp7-del7.12_behavioural-biometric_profiling_and_transparency_enhancing_tools.pdf