# Privacy-friendly Identity Management in eGovernment

Xavier Huysmans

K.U.Leuven ICRI, Sint-Michielsstraat 6 B-3000 Leuven - Belgium
xavier.huysmans@law.kuleuven.be

**Abstract.** This paper starts from the empirical finding that privacy principles are not rated very high in current eGovernment architectures. This is problematic because it leads to a substantial *privacy erosion* and undermines the existing power relations between a government and its citizens with regard to a particularly valuable asset: *personal data.* Precisely because of these power relations, there are very few incentives for government managers to implement Privacy-Enhanced Identity Management Systems *on a large scale* in an eGovernment architecture. Hereafter we introduce a less far-going alternative to Privacy-Enhanced Identity Management in eGovernment: "Privacy-Friendly Identity Management". We conclude with a brief analysis of one important driver for government managers to choose for Privacy-Friendly Identity Management: *risk management.*

## 1 Introduction

A recent field study performed in assignment of the Danish government on the usage of privacy enhancing technologies shows that across Europe, today's governmental processes only include limited **privacy protecting functionality** [19]. Also, where governmental processes are re-engineered to eGovernment services, these new developments seem to follow this trend by not rating **privacy principles** high in the basic architecture design.

In the article "Implications of profiling practices on democracy and rule of law" by [10] we read that **personal data** plays a very important role in regulating the power balances between the citizen and his/her government. Finally, as we will see below, **personal data** is a strategic resource for eGovernment.

If we tie these 3 elements together it is not unreasonable to state that a *potential* large scale usage, aggregation, exchange, data mining,... of personal data in eGovernment *may* have a negative impact on the power balances between the citizen and the State and result in privacy erosion. Several scenarios can be imagined to tackle this privacy erosion varying from blunt acceptance ("you have zero privacy, get over it")[1]

[1]Famous words spoken by SUN's CEO Scott McNealy in Jan 1999 (http://www.wired.com/politics/law/news/1999/01/17538) They illustrate an interesting approach to deal with the mentioned erosion that focuses on transparency and

*Please use the following format when citing this chapter.*

Huysmans, X., 2008, in IFIP International Federation for Information Processing, Volume 262; The Future of Identity in the Information Society; Simone Fischer-Hübner, Penny Duquenoy, Albin Zuccato, Leonardo Martucci; (Boston: Springer), pp. 245–258.

As Mr. Lessig explained in his book "Code version 2.0", *code* can be used to implement privacy features [4].

Current research on the topic of identity management and privacy, such as the EU funded PRIME project[2]

In this paper we explain that this might be a tad too much for eGovernment, because (1) privacy is not an absolute right, (2) the existence of competing interests in eGovernment and (3) of the general lack of incentives for governments to restrain their technical capabilities on the personal data they are processing.

The underlying idea (which is not further developed in this paper[3]

Before that, we first explain what eGovernment, identity management and privacy / data protection in IDM for eGovernment is about (sections 2, 3 and 4) and clarify the terms *FIDIS type 1* and *type 3*).

In the European research project FIDIS, researchers came to the conclusion that there are three main types of IDM systems, namely:

- the ones used for account management (FIDIS type 1), in which case we can speak of an assigned identity.
- the ones used for profiling of user data (FIDIS type 2) and
- the ones used for user-controlled context-dependent role and pseudonym management (FIDIS type 3).

---

accountability: don't put too much energy in keeping your personal information unknown to the world – make sure instead that you can verify what is being done with it (transparency) and hold people accountable if needed. See [17], to legal constructs (e.g., qualifying privacy as a sort of intellectual property right which can be negotiated and traded) and technical measures. It is this third approach we are writing about here.

[2]PRIME develops a *privacy enhancing identity management system* (PE-IMS), which means that via the PRIME tools, the user is empowered to decide on the release of data and on the degree of linkage to his or her personal data within the boundaries of legal regulations. More information on the PRIME project can be found at http://www.prime-project.eu, usually suggests to implement code in the identity management (IDM) architecture in a *privacy enhancing* way, which means that the IDM architecture is (1) user centric and (2) focuses on context-dependent role and pseudonym management.

[3]It is work being done in Work Package 16 of the EU funded Network of Excellence, FIDIS (http://www.fidis.net) is that it is possible to outline and fully describe the requirements of:

- an organizational IDM system (FIDIS type 1)[4]
- that especially addresses the interest of natural persons to control, or at least significantly influence the processing of data about him/her-self, and
- incorporates at least some degree of privacy and data protection requirements in the basic IDM architecture design.

We've provisionally called this a "privacy-friendly" IDM system. In section 5 of the paper we further explore the reasons why government managers should implement privacy-friendly IDM systems in their basic eGovernment architecture design.

These three types have been consolidated in the FIDIS academic community and accepted as a final deliverable by the European Commission (FIDIS deliverable 3.1 referenced below).

## 2 eGovernment

There are probably as many definitions of the term eGovernment as there are people working in that field. The definition used in Belgian federal eGovernment runs as follows:

"eGovernment is the continuous *optimization of service delivery and governance* by transforming internal and external relationships through technology, internet and new media" [8]. This optimization relies on a number of important principles. We only mention the two most important ones here.[5].

The first principle is that information shall be treated as a *strategic resource for all government activities.* On the Belgian Federal level this means, for instance, that information [8]:

- shall be modelled in a flexible way that maximally takes into accounts the users' needs.
- should be managed efficiently during its whole life-cycle. This means, inter alia, that information should be collected only once and maximally reused. In addition, a functional task division should be agreed on, to know which government entity *stores which data in authentic form.*
- information should be exchanged electronically where possible, based on a functional and technical interoperability framework and on the usage of common identification keys for all relevant entities.
- information should be processed in accordance with privacy and data protection regulation, and, more in general, be consistent and properly embedded in the law.

The main idea behind the mentioned *authentic storage of data*, is that government bodies should not collect the same information repeatedly from citizens or companies: The relevant data is collected only once and than verified, validated, stored and updated when needed.

From then on, other entities are supposed to request the information they need from these data repositories only. The government entities that are responsible to maintain these data repositories, commonly called "authentic sources", are "data managers". Data managers shall only communicate authentic data to the thereto authorized entities.

[5]Our description is mainly based on [8, 2], the federal portal (http://www.belgium.be) on the page 'about eGovernment' [14, 9]

If the data maintained in the authentic source is personal data (i.e. any information relating to an identified or identifiable natural person[6]), their disclosure is strictly limited due to privacy and/or data protection requirements.

A second important principle is the *integration of back-offices*. The term refers to the idea that government services are delivered in two phases. First the intake of the basic data for the service delivery, and a first part of the service delivery by the front-office (e.g., a government website), and then the completion of the service by the back-office [2].

The back-office evaluates if the client[7] is entitled to get the service or not, verifies the data received from the client at other entities, and/or communicates them to other entities. A large part of the service process is not visible by the client and should not necessarily be performed by the same government entity.

It can be performed by several departments of several administrations from different government levels, working together in some form of cooperation structure [2]. The result of the service process is presented to the client via one or more front-offices.

From a technical perspective the integration of back-offices is typically looked for through a (cross-border) "*Service Oriented Architecture*"(SOA).

In practice, identity management components (such as authentication services) are often integrated as basic service components of such a SOA in eGovernment. These services are then compiled with other services to so-called value-added services [15].

## 3 Identity Management in eGovernment

Identity Management (IDM) is the definition, designation and administration of identity attributes as well as the administration of the choice of the partial identity to be (re-) used in a specific context, to manage the access to and the usage of online applications, services and resources [18, 12][8].

It includes the management of identity attributes by their owners (user-side IDM) and/or by those parties with whom the owners interact (services-side IDM). The infrastructure used for the definition, designation and administration of these identity attributes is the identity management system.

There are several strong drivers to implement Identity Management (IDM) in eGovernment, such as, for instance:

[6]Art. 1 Directive 95/46/EC of the European Parliament and of the Council of 24 Oct 1995 on the protection of individuals with regard to the processing of personal data on the free movement of such data, Official Journal of the European Communities, L 281, 23 Nov 1995, 31-50.

[7]As explained in section 3.1 of FIDIS deliverable 5.4 (in press), the notion to see a citizen as a client of the "business of government" was introduced a few decades ago. It is strongly present in current Belgian eGovernment, where citizens and enterprises are being treated as government's clients (see for example the used terminology on the federal portal (www.belgium.be) (in the section "about eGovernment")).

[8]Definition from Wikipedia, available at: http://en.wikipedia.org/wiki/Identity_management.

- a reduction of the cost of the organization's system (e.g., optimization of user management via account creation),
- an increased efficiency, transparency and effectiveness of the organization's activity,
- an improvement of the functionality or experience (e.g., via single sign on), and
- a reduction of the operational risk of the organization's activity.

There are also a number of good reasons for not implementing IDM systems in eGovernment. IDM systems rely on input from many different areas and levels both within, across and potentially from outside the organization. Their implementation is not an easy task. In addition, it is also clear that the usage of IDM systems creates additional risks (for example because of the cross-context exchange of personal data, which implies additional data protection and privacy risks and the additional exposure to security risks).

Depending on the goals of the eGovernment project, it is usually good to start with a risk assessment of the organization's activity. Such an assessment starts with the evaluation of the need for identity management mechanisms to protect information, applications and the infrastructure of the organization.

These mechanisms can be understood in terms of a lifecycle: (1) create an identity of an entity, (2) authenticate the identity, (3) grant the appropriate permissions to that entity, (4) monitor and incorporate accountability mechanisms, and finally (5) audit and assess the IDM processes [16].

In order to perform this lifecycle, we typically need the following components of an IDM system:

- registration,
- identification,
- authentication,
- authorization and access control,
- user management,
- accountability,
- audit, and
- data storage and communication.

Not all IDM systems contain all these components. It is also important to realize that, since they are all part of the mentioned lifecycle, they are also strongly interconnected.

In sum, we can conclude that in eGovernment identity management is an integral part of the general data management architecture of a SOA where identity management mechanisms help:

- to manage risks (e.g., operational risks related to unauthorized disclosure of personal data etc.),
- to enhance trust and
- to provide more efficient, more secure and more effective services to the government's clients (citizens, businesses etc.).

## 4 Privacy and data protection in identity management for eGovernment

The implementation of IDM in eGovernment can, but does not necessarily take into account privacy and/or data protection requirements.

As mentioned in the introduction section, when governmental processes are being re-engineered to eGovernment services, *privacy principles are often not rated high in the basic architecture design.*

There are a number of good reasons why this is problematic, especially in eGovernment. One of them is that the usage of ICT in governmental processes creates new, substantial risks, which should be adequately answered *to maintain the power balance between the citizen and the state with regard to personal data.*

Indeed, one should not forget that the fundamental right to privacy[9] protects the fundamental political value of a *democratic constitutional state.*

This means that it guarantees individuals their freedom of self-determination, their right to be different and their autonomy to engage in relationships, their freedom of choice, their autonomy as regards for example - their sexuality, health, personality building, social appearance and behavior, and so on.

With other words, privacy guarantees each person's uniqueness, including alternative behavior and the resistance to power at a time when it clashes with other interests or with the public interest. It therefore plays an essential role in *regulating the power balance* between governments and their citizens in regard to a very important government' resource: information [10, 3, 2].

When privacy and data protection requirements are left out from the IDM architecture, the latter typically includes *user identification*, and data exchange is typically based on the common usage of *globally unique* identification keys.[10]

This creates important risks: when personal data from one context can be linked to personal data from another context (internal or external to the government sphere), it *can* result in detailed profiles about natural persons and a significant lack of privacy. Even though such interconnections can be unauthorized or illegal, it is not excluded that they will take place anyway.

The key question we have to ask ourselves is therefore whether – to protect the fundamental right to privacy and to make sure the European data protection principles are being respected – it suffices to rely on procedures to be applied by the administrative staff, if, at the other hand, massive data aggregation and

[9] which was codified, inter alia, in article 8 of the European Convention on Human Rights and article 22 of the Belgian Constitution

[10] This is for example the case in Belgium, where data exchange mainly relies on the usage of the National Registry Number of the person to whom the exchanged data relates. Since decades, a unique identifier is being assigned to Belgian citizens at their first registration in the National Registry. Since the advent of Belgian eGovernment, this identifier has become *globally* unique because it is now used to refer to that person *across several government contexts.* It is thus not limited to one or more particular spheres of government' activity. Other "relevant" entities (such as enterprises, foreigners etc.) hold a similar, globally unique identifier.

linkage of databases is at least being facilitated through the unrestrained usage of ICT in eGovernment.

We believe the answer is no. We are convinced that if a substantial erosion of privacy is made possible through eGovernment, governments must take all necessary countermeasures, including technical ones. We will come back to this below.

As mentioned supra, several approaches to counter such a privacy erosion can be imagined. Research on the topic of privacy and identity management often suggests to tackle privacy erosion through a translation of privacy and/or data protection rules into code (cf. ideas by L. Lessig) [4].

Yet, research that aims at incorporating privacy and data protection rules in the IDM architecture also usually focuses on *maximum privacy*. The enhancement from a privacy perspective is mainly based on the notion that the protection can and should be put in the hands of the person the user trusts most: *himself*.

A privacy-enhancing application design therefore supports both "user-controlled data release" as well as "user-controlled data linkage" [13].[11]

Discussions we've had with government managers so far seem to indicate that this type of privacy enhancements may be over-ambitious for eGovernment. They do not see enough incentives to implement such an IDM system *on a large scale* for systematic exchange of personal data in eGovernment.

This is understandable to some extent, because privacy is not an absolute fundamental right: not one single aspect of privacy takes absolute precedence over other rights and interests. Never does an individual have absolute control over an aspect of his/her privacy.[12]

Privacy can thus be restricted when balanced against other interests (rights of others, law enforcement, public health, etc.) and under a number of conditions

[11]This $29^{th}$ edition of this terminology paper makes an explicit distinction between user centric privacy enhancing identity management, and (general) privacy enhancing identity management. Contrary to the above mentioned PRIME project, the latter does not include user centricity as such. It focuses on unlinkability as a privacy enhancing technology. In Prof. Pfitzmann and Mrs. Hansens's view, a Privacy-Enhancing IDM system can therefore be defined as an IDM system that, given the restrictions of a set of applications, sufficiently preserves unlinkability (as seen by an attacker) between the partial identities and corresponding pseudonyms of an individual [13]. Although we can in principal agree to take user centricity out of the definition of (general) PE-IDM, it would lead us too far to further go into detail on these terms here. More information on that topic, however, can be found in the deliverables of WP16 of the FIDIS project.

[12]This is nicely illustrated by the fact that the European Court of Human Rights (ECHR) recognizes different sorts of human rights. The ECHR recognizes some so called 'hard core' or absolute rights that must be respected even in times of emergency when derogations to other rights are justified (article 15 2 ECHR). Next to this there are 'normal rights' (e.g., article 5 and 6 ECHR) which can be derogated from in times of emergency (article 15 1). Finally the ECHR counts four rights which can be legitimately restricted in terms of emergency but also under some specified conditions (article 8-11 ECHR, the conditions for permissible restrictions are listed in the second paragraphs of these Articles). Privacy is one of these 'restrictable rights'. See [10].

(such as, the legality of the restriction, the link with a pressing social need and the proportionality between the restriction and these needs) [6].

Tasks government entities carry out in the public interest undoubtedly justify to some extent limitations of the right to privacy and the foreseen exceptions of the general data protection rules.

It is self-evident that these exceptions and limitations also effect the privacy components of a data and identity management architecture used in eGovernment. Concretely, this means that a privacy-enhanced (or maximised) identity management architecture which implements *user-controlled context-dependent role and pseudonym management* will often not be a realistic option in eGovernment, where privacy coexists with a number of strong other interests and exceptions.

This does not mean, however, that there is no alternative available. The underlying idea – which is not further developed here – is that there are indeed less far-going ways to increase privacy and data protection through code in eGovernment. The research objective is obviously not to be only compliant with privacy and data protection regulation, but where possible also to go one or more steps beyond and thereby re-equilibrate the power balance between the citizen and the State.

Explained in terms of the types of IDM systems set out in deliverable 3.1 of the FIDIS project [5], we believe there is concrete research to be done in investigating privacy enhancements of a type 1 IDM system (i.e., services-side and used inter alia for accounting and user management) in eGovernment instead of putting the focus on a type 3 IDM system.[13]

## 5 Why privacy friendly IDM in the basic architecture used in eGovernment?

Even though there might be a lack of drivers to implement a IDM system that focuses on maximum privacy on a large scale in eGovernment (PE-IMS, as described above), there are very good reasons to incorporate at least some degree of privacy and data protection requirements in the basic data architecture design used in eGovernment. These drivers are, for example:

- the reduction of the operational risk of the organization's activity due to data protection and privacy requirements,
- an increased trust in the eGovernment project, since users get more transparency and a way to enforce their privacy and data protection rights,
- the auditability of compliance with the regulation and/or authorizations received to exchange a particular set of data.

We believe these and other drivers need to be made explicit via research, to be convincing enough for government managers to change some of their priorities on privacy and data protection in eGovernment.

[13] FIDIS type 3 IDM systems typically include user-controlled context-dependent role and pseudonym management.

For the limited purposes of this paper, we believe it is useful to say a few words on the first driver we've pointed out: *risk management.*

Risk is a well-known concept in the industry, but is less known in a government context. It can be defined as the likelihood that an unwanted incident will occur and the impact that could result from the incident [21]. Its basic principles can be summarized as follows:[21, 11].

- Both businesses and governments have to achieve well-known objectives, within a well-known context of acceptable risk.
- Sustainable results can only be achieved when both industry and operational risks are being managed and thus kept under control.
- Industry risk refers to the risk inherent to the performed activities (e.g., the customer insolvency for a bank).
- Operational risk refers to the risks caused by inadequacy or failure in the day to day business (e.g., illness of the personnel, theft of goods, non-compliance with legislation etc.).

Organizations that manage their industry and operational risks assess what the loss might be if something goes wrong, and whether they can absorb that loss if it indeed goes wrong. These decisions are typically based on information provided by trusted third parties (audits etc.). Risk assessment is the process of identifying and evaluating such risks.[21, 11].

Managing risks thus leads to concrete actions, for example subscribing insurances, the provisioning of sufficient financial means or accepting risks and communicating these decisions to the stakeholders.

Operational risks very often result from legal or sector-specific obligations. For example, in the banking sector, banks are forced to provision a large part of the money they dispose of to contain the risk of bankruptcy. Other obligations for example arise from privacy and data protection regulation.

If we accept that the unrestrained usage of ICT in eGovernment at least potentially creates a substantial risk of privacy erosion for the persons to whom the data relates, this is an operational risk that needs to be identified, and which should result in a concrete *risk decision.*

A risk assessment of an eGovernment project could for example result in the decision to accept the risks related to a potential eGovernment "privacy-gate scandal" and the negative publicity, court cases, loss of electorate, burning decisions of the privacy commission etc. that goes with it.

We do not think it would be a wise decision to just accept that risk, because of the *objective liability provision* contained in the data protection regulation.

Before we go any further, we need to explain 3 legal rules:

1. *Objective risk liability:* Article 23 of the European Data Protection Directive, as transposed in article 15bis of the Belgian Data Protection Act[14] states

[14]Law of 8 December 1992 on Privacy Protection in relation to the Processing of Personal Data, Belgian State Gazette 18 Mar 1993, as modified by the law of 11 December 1998 implementing Directive 95/46/EC, Belgian State Gazette 3 Feb 1999, and the law of 26 Feb 2003, Belgian State Gazette 26 Jun 2003.

that *the data controller* – this is the entity that alone or jointly with others determines the goals and the means of the processing of personal data – *is in principle liable for the damages caused to the data subject as a result of a processing or any act that is not compatible with the Data Protection legislation.* He may only be exempted from this liability, if he proves that is not responsible for the event that gave rise to the damages. This is an exception to the normal liability rules, following which, to hold someone accountable, one has to prove the existence of a fault, damages and a causal link between them (art. 1382 of the Belgian Civil Code).
The mentioned data protection article is an "objective" risk liability provision, because there is no need to prove the fault of the data controller to hold him/her accountable for a certain action: the mere fact that he/she infringed the data protection law leads to liability, of course only if there is a causal link between the damages and this infringement of the law.

2. *Privacy in the data protection law:* Article 2 of the Belgian Data Protection law introduces a subjective right for natural persons to *respect for their private life* (read: privacy) *with regard to the processing of personal data that concern him/her.*
Similarly, article 1 of the Data Protection Directive states that *Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.*[15].
Concretely, based on this article, one can say that the obligation to respect the right to privacy is also applicable to data controllers. We will come back to this below.
3. *Obligation to take the appropriate technical and organizational measures:* Article 16 of the Belgian Data Protection Law and article 17.1 of the Data Protection Directive contain an obligation to take *appropriate technical and organizational measures* to protect the processed personal data against:
   - accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and
   - *against all other unlawful forms of processing.*

   Such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected, having regard to the *state of the art* and the cost of their implementation. The Belgian article further specifies to whom it applies (inter alia to data controllers) and foresees the possibility to explicate these obligations by means of a Royal Decree.

By jointly reading these 3 legal rules, it becomes clear that, (1) if we accept the fact that the unrestrained ICT usage in eGovernment at least potentially

[15]The main difference between both texts is that only the Belgian article creates a concrete (subjective) right for natural persons which is usable in court to tackle infringements committed by other natural persons. This is the so-called horizontal action of the right to privacy. Both texts apply, however, also to vertical relations between governments and the natural persons that fall under their jurisdiction.

creates a substantial risk of privacy erosion for the persons to whom the data relates and (2) if a government wants to avoid the mentioned liability risk, all adequate organizational and technical measures should be taken to avoid unlawful forms of data processing, which also means having respect for the privacy regulation mentioned in section 4 (second bullet point).

Also, as explained in the third bullet point, the "adequateness" of such measures is evaluated by having regard to the state of the art. The latter could, *given the maturity of the research on privacy and identity management*, refer to the incorporation of at least some degree of privacy and data protection in the basic eGovernment architecture design.

If an eGovernment architecture does not take such privacy enhancing measures into account, one should realize that – in case something happens –, data controllers or entities acting on their behalf can be held accountable, *even without a concrete or proven fault*, if it appears that the eGovernment architecture was not adequate to protect the personal data at stake.

Whether a concrete IDM architecture is adequate or not is easy to evaluate. Nevertheless, it is clear that the usage of privacy enhancing *technologies* are increasingly being perceived – also on the political level – as a suitable way to enhance the level of privacy and data protection in an organization's activity.[16]

In sum, to answer the question asked before, namely whether it suffices to rely on procedures to be applied by the administrative staff, if, at the other hand, massive data aggregation and linkage of databases is at least being facilitated through the unrestrained usage of ICT in eGovernment.

We believe the answer is NO, because it becomes more and more likely that Privacy Enhancing Technologies are necessary to comply with the above mentioned obligation to take all appropriate technical and organizational security measures.

## 6 Conclusion

The starting point of this paper was the establishment of two facts: first, that the unrestrained usage of ICT in eGovernment creates a substantial privacy erosion and second, that privacy principles are often not rated very high in a basic eGovernment architecture design.

The question we asked ourselves is whether – to protect the fundamental right to privacy and to make sure the European data protection principles are being respected – it suffices to rely on procedures to be applied by the administrative staff, if, at the other hand, massive data aggregation and linkage of databases is

[16] See for instance, the recent communication of the European Commission on the Promoting Data Protection by Privacy Enhancing Technologies (PETs) on this topic: *"To pursue the objective of enhancing the level of privacy and data protection in the Community, the Commission intends to clearly identify the need and technological requirements of PETs and further promote the development of these technologies* [...] *and their use by industry and public authorities, involving a vast array of actors, including its own services, national authorities, industry and consumers."*[17]

at least being facilitated through the unrestrained usage of ICT in eGovernment. The goal of this paper is to explain why we believe this is not the case.

After a general introduction on eGovernment and identity management (sections 2 and 3), we explained that there are several approaches to tackle this privacy erosion and that research on privacy and identity management that wants to implement privacy and data protection *via code*, usually focuses on *maximum privacy*. This means that it usually includes *user-controlled data release and user-controlled data linkage via context-dependent role and pseudonym management.*

We explained that this might be a tad too much for eGovernment, because (1) privacy is not an absolute right, (2) there are a number of valid, competing interests in eGovernment and (3) there seem to be a general lack of drivers for governments to restrain from technical capabilities on the personal data they are processing.

We suggested to follow another approach to implement privacy and data protection requirements in the basic eGovernment architecture design. We made clear that there is concrete research to be done in investigating privacy enhancements of an organizational IDM system (i.e., services-side and used inter alia for accounting and user management, also called FIDIS type 1) in eGovernment.

The Privacy enhancements as such were not described in the paper. We only pointed out that such enhancements would probably have to (1) especially address the interest of natural persons to control, or at least significantly influence the processing of data about him/her-self, and (2) integrate at least some degree of privacy and data protection requirements in the basic IDM architecture design.

In the last section of the paper we identified a number of reasons to choose for a so-called "privacy-friendly identity management system" which does exactly that. One of these reasons is *operational risk management.*

We've explained that – from a risk management perspective – the obligation to take *adequate* organizational and technical measures is a strong driver to implement a "privacy-friendly IDM system".

Indeed, the adequateness of such measures is, inter alia, evaluated by taking into account the state of the art. The latter could, given the maturity of the research on privacy and identity management, refer to the incorporation of at least some degree of privacy and data protection in the basic eGovernment architecture.

In our view, it would therefore definitely be a too large risk to take, to only rely on procedures to be applied by the administrative staff to protect privacy and to make sure the European data protection principles are being respected in eGovernment.

## References

1. Boutonnet M. Le Principe de Prcaution en Droit de la Responsabilit Civile, Librairie Gnrale de Droit et de Jurisprudence, Paris, 2005.

2. De Bot D. Privacybescherming bij e-government in België – Een kritische analyse van het Rijksregister, de Kruispuntbank van Ondernemingen en de elektronische identiteitskaart. Vandenbroele, Brugge, 2005.
3. De Bot D. Verwerking van persoonsgegevens, Kluwer, Antwerpen, 2001.
4. Lessig L.Code version 2.0. Basic Books, New York, 2006.
5. Bauer M., Meints M., and Hansen M. Fidis Deliverable 3.1., Available at: http://www.fidis.net 15 Sep 2005, last visited: 20 Aug 2006
6. Buchta A., Dumortier J., and Krasemann H. The Legal and Regulatory Framework for PRIME, in FISHER-HUEBNER S, ANDERSSON CH and HOLLEBOOM TH (eds.), PRIME D 14.1.a: Framework V1, Available at: https://www.prime-project.eu/prime_products/reports/fmwk/pub_del_D14.1.a_ec_wp14.1_V4_final.pdf, 13 Jun 2005, last visited: 13 Jun 2005.
7. De Hert P. Titel II De Wet 8 Dec 1992 met betrekking tot de verwerking van persoonsgegevens, Apr 2005, in P. DE HERT (ed.), Privacy en Persoonsgegevens, Politeia, Brussels, 2005.
8. Deprest J. and Robben F. eGovernment: the approach of the Belgian federal administration. Available at: http://www.ksz.fgov.be, Jun 2003, last visited: 20 Jun 2006
9. Deprest J. and Strickx P. eGovernment initiatives. Available at: *http : //www.ibbt.be/egov/pres/9.janDeprest_2005.10.26 −e Govupdatei nitiatieven.ppt*, 26 Oct 2005, last visited: 20 Sept 2006
10. Hildebrandt M., Gutwirth S., and De Hert P. Fidis Deliverable 7.4, Implications of profiling practices on democracy and rule of law, Available at: http://www.fidis.net, 5 Sep 2005, last visited: 15 Sep 2006.
11. Huyghens C.H. IDM in the risk universe, liability, methodology, standards, Available at: https://projects.ibbt.be/idem/uploads/media/2005.12.20.idem.workshop1.risk.pdf, 20 Dec 2005. last visited: 20 Dec 2005.
12. Leenes R. and Fischer-Huebner, S. PRIME Framework version 2. Available at: http://www.prime-project.eu, Jul 2006, last visited: 23 Aug 2006
13. Pfitzmann A. and Hansen M. Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management - A Consolidated Proposal for Terminology. Version 0.29. Available at: http://dud.inf.tu-dresden.de, Jul 2007, last visited: 31 Jul 2007
14. Robben F. eGovernment, presentation available at: http://www.law.kuleuven.be/icri/frobben/presentations/20060327b.ppt, 27 Mar 2006, last visited: 1 Apr 2006.
15. Robben F. E-government in the Belgian social sector coordinated by the Crossroads Bank for Social Security, presentation available at: http://www.law.kuleuven.be/icri/frobben/presentations/20060623nl.ppt, 23 Jun 2006, last visited: 22 Mar 2007.
16. Slone S. Identity Management. A white paper. Available at: http://www.opengroup.org, Mar 2004, last visited: 11 Nov 2004
17. Weitzner D, et al. Transparency and End-to-End Accountability: Requirements for Web Privacy Policy Languages', A position paper for the W3C Workshop on Languages for Privacy Policy Negotiation and Semantics-Driven Enforcement, available at: http://www.w3.org/2006/07/privacy-ws/papers/, Oct 2006, last visited: 17 Oct 2006.
18. Identity Management Systems (IMS). Identification and Comparison Study', Available at: http://www.datenschutzzentrum.de, Sep 2003, last visited: 7 Jul 2005

19. Report on Privacy Enhancing Technologies, performed for the Danish Ministry of Science and Innovation. Available at: http://www.vtu.dk/fsk/ITC/Rapportvedrprivacyenhancingtechlologies.pdf, 28 Mar 2005, last visited: 15 Oct 2005
20. Modinis IDM Terminology Paper, Available at: https://www.cosic.esat.kuleuven.be/modinis-idm/, 23 Nov 2005, last visited: 22 December 2005
21. IDA Authentication Policy. Basic policy for establishing the appropriate authentication mechanisms in sectoral networks and projects, Available at: http://ec.europa.eu/idabc/servlets/Doc?id=19281, Jul 2004, last visited: 20 Oct 2006.