Privacy by design and administrative efficiency in e-governance

Vanderose, Benoît; Degrave, Élise; Habra, Naji

Published in:
CEUR Workshop Proceedings

Publication date:
2015

Document Version
Publisher's PDF, also known as Version of record

Privacy by Design and Administrative Efficiency in E-Governance: a Case Study

Benoît Vanderose, Élise Degrave, and Naji Habra

University of Namur
{benoit.vanderose,elise.degrave,naji.habra}@unamur.be

Abstract. Achieving administrative efficiency is one of the objectives pursued by e-governance. Many aspects of government to citizen and government to business exchanges may be streamlined through an adequate use of information and communication technologies (ICT). However, among the various challenges facing e-governance, legal issues regarding data protection and privacy are often perceived as curbing the full potential of ICT regarding efficiency. In this paper, we introduce a decentralized information management model used for the development of e-government in Belgium and that illustrates how privacy and efficiency dot not have to be opposing forces. We discuss the key aspects of this model and how it complies to the principles of a privacy by design approach. We assess its overall strengths and weaknesses as well as its potential to support further legal requisites such as the right to information and transparency.

Key words: Privacy by design, administrative efficiency, information management model, case study

1 Introduction

Achieving administrative efficiency sits among the core principles underlying the implementation of good governance and e-governement [11].

Attempts to provide better tools to support administrative decision-making [3], to improve software development processes in public administrations [1] or to investigate how to increase user satisfaction whilst decreasing administrative burden [12] contribute to a more efficient organisation of public administrations.

A central aspect of administrative efficiency lies in how data pertaining to citizens are managed, acquired and made available. Choosing a relevant strategy regarding the management of citizen-related information may offer important improvements in usability and efficiency. For instance, the reuse and sharing of previously acquired data among different administrations allows a decrease of administrative burden for this particular citizen (i.e., not to be forced to provide the same piece of information multiple times since the data is shared and reused).

However, inherent risks of administrative simplification lie in oversimplification of the design of the envisioned strategy. Typically, a straightforward design

to support sharing and reusing citizen-related information would be to implement a centralized information management model with a central data source that would gather every piece of information pertaining to citizens and all aspects of their citizenship (e.g., vital records, health-related data, etc.). Such a model has already been proposed in the past. For instance, the Automated System for Administrative Files and the Repertory of Individuals (SAFARI) [2], was proposed by the French government during the seventies and embodied such a centralised information model. Of course, this strategy raised a lot of concerns regarding privacy protection and security that led to the dismissal of the project.

This example illustrates how important it is to take the requirements of privacy protection into account during the early stages of a project (especially related to e-governance). If possible problems of privacy protection are discovered during the early stages of a project, they may be analysed and integrated to the design process in order to avoid future failure. This approach, known as "Privacy by Design" (PbD) [10], is also a way to avoid the possible conflict between privacy and efficiency since it emphasizes a user-centric approach that naturally impacts the usability of the designed strategy.

In order to contribute to an effort of much needed [7] consolidation in e-government, we studied the global strategy and information management model regarding citizen-related data that is being deployed in Belgium. We looked at what the key aspects are that guarantee its functionality and how it satisfies most privacy protection measures while guaranteeing an increased efficiency from a user-centric point of view.

The remainder of this paper is organised as follows. Section 2 discusses different strategies regarding the management of citizen-related information. Section 3 describes the Belgian e-governance information management model. Finally, Section 4 discusses the assessment of this model whilst Section 5 provides some closing comments.

2 Managing citizen-related information

The core of e-governance lies in the management of large amounts of sensitive citizen-related information. Managing this information constitutes the back-office of administration. Furthermore, this information is related to many aspects of the citizen's life (e.g., identification, health, vehicle registration, etc.) and is therefore extremely sensitive and critical privacy-wise. Risks associated to the administration collecting this much data on citizens are multiple. First, possessing this much information makes it possible for unauthorized public servants to cross-check private information (e.g., checking the name associated to a plate number and using this information to track the address of one individual). This explains why a centralized information management model raises concerns: it would simply make such an abuse of the data much easier.

Decentralization offers the possibility to make this cross-checking more challenging for unauthorized users (provided that some precautions are taken as explained in Section 3) but raises different concerns.

In [7], the authors provide a comparison of various European countries regarding their global e-government implementation strategy and more specifically in the strategy regarding the back-office. It shows that mainly two models are possible: a model relying on the concept of authentic data source (such as the model described in Section 3) and a model relying on the notion of digital vaults. A digital vault is a secured data storage that is provided to every citizen to store every relevant personal data. This model may be viewed as a centralized model *at the citizen level*. In fact, it has been much criticized regarding the security risks and privacy concerns that it raises [8].

Finally, one risk that is often understated or disregarded in the field of governance and public administration is the fact that its inherent complexity may prevent adequate control and introduce errors. Basically, in a constantly evolving world, the citizen gradually lose track of what information different public services may posses about her or even if this information is correct [5]. In [8], the idea of a citizen-centric information portal is described as a solution to provide "effective, efficient and transparent electronic government services". However, such a portal inherits the problems of the back office and must therefore be implemented on the basis of a sound strategy and information management model.

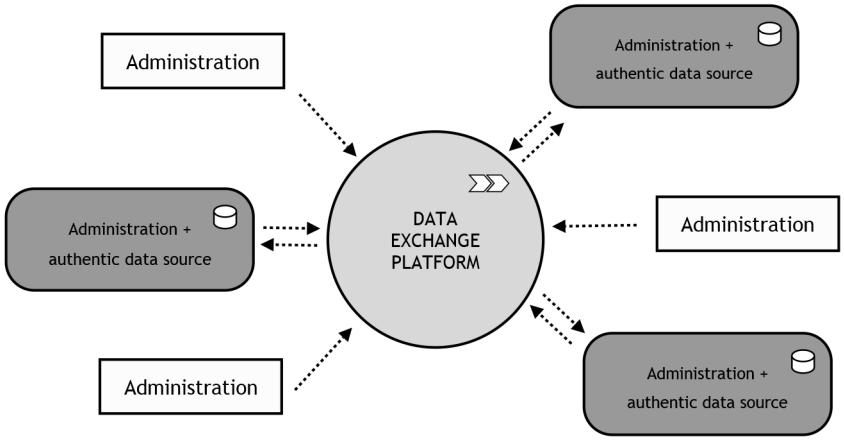

Fig. 1. Global overview of the Belgian e-governance information management model

3 Belgian e-governance information management model

The Belgian e-governance strategy regarding information management relies on a decentralisation across two dimensions. The first dimension relates to the fragmentation of the back office into different sectors of the pubic administration (e.g., social security status, business information, car registration, etc.). The

back-office of the Belgian e-government therefore constitutes a series of networks dedicated to specific aspect of the citizen-related information.

For each **sector-specific network**, the model is based on a decentralised organisation of data consumers (i.e., public administrations) and data providers (i.e., the so-called authentic data sources) as illustrated in Fig. 1.

The concept of **authentic data source** is key to this architecture. An authentic data source is a database managed by an administration. This administration is appointed through a legal directive with the responsibility and ownership of the type of data stored in the database. This administration therefore manages all aspects (acquisition, storage, update, destruction, security) of a specific type of information regarding the citizens. The legal prescription on authentic sources also prevent any other public administration from gathering this specific type of information.

If another administration of the same sector-specific network needs access to this specific type of data, it will do so through a **data exchange platform** referred to as 'crossroad banks'. Despite a misleading name, those crossroad banks are not databases per se but actual hubs of data that allows the integration of different authentic sources. They act as information brokers between consumers and producers (authentic sources).

Finally, citizens are associated with **identification numbers** that are specific to the sector-specific network. These identification numbers allow the crossroads banks to redirect the relevant information to the right data consumer.

4 Assessment of the model

In order to assess the model presented in Section 3, we compared it to an approach based on digital vaults and took 2 quality aspects in consideration: administrative efficiency and compliance to privacy principles.

Regarding *administrative efficiency*, two sub-characteristics are to take into account: the ease of use (citizen point of view) and the decrease of administrative burden (administration point of view). Both may be considered as one-dimensional quality for which satisfaction and level of fulfilment are proportional [9]. From the citizen point of view, the model fulfils the usability as much as a vault-centric approach. Indeed, the citizens are not forced to provide the same information multiple times and their data is verified and reliable across the sector-specific network. From the administration point of view, both approaches offer a similar level of fulfilment in avoiding the multiplication of conflicting data sources for a single piece of data. Vault-centric approaches and the Belgian information model offer the same advantages regarding the administrative efficiency.

Regarding *compliance to privacy principles*, the discussed model provides clear advantages compared to vault-centric approaches. First, there exists no central database that may be abused to gather every aspect of a citizen's life. Besides, the identification number associated to a citizen is unique to each sector-specific network and prevents cross-checking of information.

Regarding the physical security of sensitive databases, the model relies on the security of the authentic data sources but, due to the decentralisation, is only as strong as its weakest link. The quality of the data infrastructure for the authentic source must therefore be guaranteed.

Mainly, the Belgian model shines in terms of protection from malicious uses inside the administration itself. Although it does not result from the explicit application of a 'privacy by design' approach, the model complies to similar principles. The seven foundational principles of Privacy by Design are formulated as follows [4]:

1. Proactive not Reactive; Preventative not Remedial
2. Privacy as the Default Setting
3. Privacy Embedded into Design
4. Full Functionality Positive-Sum, not Zero-Sum
5. End-to-End Security Lifecycle Protection
6. Visibility and Transparency
7. Respect for User Privacy

The information management model implicitly complies to these principles. Privacy has been embedded in the basic requirements and influenced the design of the model, therefore making privacy protection the default setting of the model (principles 1-3).

There is no trade-off regarding the usability (principles 4 and 7) and since authentic data sources are the only one allowed to hold a given piece of information, control over data lifecycle is guaranteed (principle 5).

However, compared to vault-centric approaches, there is no possibility for the citizen to view the sum of all information possessed by the public administration (principle 6). As pointed in [5], this is one risk that must be tackled in the future. However, the decentralised nature of the model makes it extensible and makes it theoretically possible to implement a citizen-centric portal that would interface directly with the crossroad banks. Such portal would inherit from the privacy advantages whilst improving and assuring further legal requisites such as the right to information and transparency.

5 Conclusion and future work

We described how a decentralised information management model based on the concept of authentic data sources is currently being implemented throughout the Belgian public sector. This model offers a number of advantages regarding the achievement of an efficient administration and quality of public services similar to other model relying on digital vaults.

Additionally, this model provides a prime example of a design that integrates by nature safety mechanisms regarding privacy-related concerns (i.e., a privacy by design approach). It avoids centralising all available data about a citizen in a single data source. The decentralised nature of the strategy offers a significant

level of extensibility which in turn provides a way to implement systems that take further legal rights into account (such as an audit trail).

However, this model is still not formalised to become a structured and repeatable methodology. Future efforts should focus on documentation and in depth analysis process. Besides, our study is currently limited to the most hight level aspects (that is the conceptual and strategic level) and privacy-related aspects of the information management model. Future work will focus on the specifics of the data architecture [6] underlying the information model so that actual blueprints and recommendations may be drawn from this case study (while investigating how privacy protection mechanisms may be enforced at lower level of abstraction).

Finally, the most promising opportunity this decentralised model offers certainly lies in the its potential to develop a citizen-centric information portal that avoids centralisation. Investigating how individual may become data consumers within the model is the next step towards a more efficient public administration. In the future, technical constraints (regarding authentication, security, etc.) should be analysed and documented while keeping this strong focus on privacy as a default setting.

References

1. Ayed, H., Vanderose, B., Habra, N.: Supported approach for agile methods adaptation: An adoption study. In: Proceedings of the 1st International Workshop on Rapid Continuous Software Engineering. pp. 36–41. ACM (2014)
2. Belen, V.: Les tentatives de protection des données personnelles des individus: difficultés de définition et risques nouveaux. Market Management 5(2), 65–80 (2005)
3. Benjamin, S.M.: Evaluating e-rulemaking: Public participation and political institutions. Duke Law Journal pp. 893–941 (2006)
4. Cavoukian, A., et al.: Privacy by design: The 7 foundational principles. Information and Privacy Commissioner of Ontario, Canada (2009)
5. Degrave, E.: L'e-gouvernement et la protection de la vie privée. Légalité, transparence et contrôle, collection du CRIDS, vol. 36. Larcier, Bruxelles (2014)
6. Inmon, W.H., Zachman, J.A., Geiger, J.G.: Data Stores, Data Warehousing and the Zachman Framework: Managing Enterprise Knowledge. McGraw-Hill, Inc. (1997)
7. Janssen, D., Rotthier, S.: How are they doing elsewhere? trends and consolidations in e-government implementation. In: annual EGPA Conference, Oeiras. (2003)
8. Janssen, W., Zeef, P.: Vision and valuation of a citizen-centric shared information portal. BLED 2006 Proceedings p. 38 (2006)
9. Sauerwein, E., Bailom, F., Matzler, K., Hinterhuber, H.H.: The kano model: How to delight your customers. In: International Working Seminar on Production Economics. vol. 1, pp. 313–327 (1996)
10. Schaar, P.: Privacy by design. Identity in the Information Society 3(2), 267–274 (2010)
11. Von Haldenwang, C.: Electronic government (e-government) and development. The European Journal of Development Research 16(2), 417–432 (2004)
12. Wauters, P., Lorincz, B.: User satisfaction and administrative simplification within the perspective of egovernment impact: Two faces of the same coin. European Journal of ePractice 4(2), 1–10 (2008)