

Enhancing Trust on e-Government: A Decision Fusion Module

Bruno Lage Srur and Valipuram Muthukumarasamy
School of Information and Communications Technology, Griffith University
b.srur@griffith.edu.au, v.muthu@griffith.edu.au

Abstract

Advancement in Information and Communications Technologies (ICT) has increased privacy concerns among citizens. In this paper we examine how interconnected modules could be developed to mitigate those concerns and foster trust among e-Government stakeholders. Current e-Government measurement models do not adequately address privacy issues. We suggest that privacy enforcements should be added as major criteria of evaluation. Moreover, users should be able to choose the level of privacy and security needed for any system interaction. Thus, a conceptual model that allows for users to easily control the selection of privacy preferences is needed. A Decision Fusion Module takes the user inputs, such as level of privacy, pseudonymity and trust, and processes them to output the best possible selection of security mechanisms corresponding to those user preferences. In fact, e-Government models could benefit from the earned user trust.

1. Introduction

Although very sophisticated security mechanisms are in place to provide data security in e-Government implementations, security breaches still occur frequently. Specially, privacy concerns among citizens are an important issue in leading e-Government countries that are customer-centric. The aim of this paper is to propose a new proactive approach which would not only comply with privacy regulations, but would also convey trust, based on the concept that Governments can earn citizens' trust. This paper has incorporated a model for security-privacy-preserving techniques in a model that gives the user more control over their preferences, supporting trust creation.

Trust has an economic value to companies and it may be used to win competitive advantages. Today,

privacy and trust have become critical aspects of any business imperative [1].

There is a strong need for e-Government models to incorporate appropriate control mechanisms in order to provide the level of privacy and security warranted in the modern networked world. Thus, increasing trust among all the e-Government stakeholders is becoming necessity.

Correct measurement practices are directly related with a better management practice. Data can be analyzed, compared hence best practices can be enforced. Current e-Government measurement models do not enforce privacy as major evaluation criteria. Privacy criteria must be added to the existing appraisal framework models, putting the emphasis on the importance that privacy represents to citizens. It has the potential to promote a better and more precise evaluation model for e-Government. Users should also be able to choose the level of privacy and security needed for any system interaction.

Furthermore e-Government models have a great potential to earn citizens' trust; therefore, a framework for privacy and trust in the e-Government context is presented. In this paper we begin with the a discussion of related work, followed by a presentation of the proposed models, analysis of the decision fusion module (DFM), and conclude with a summary of the proposed recommendations and future research and development requirements.

2. Related work

E-Government is the use of information technology, specifically the Internet, to enhance the access to and to deliver Government information and services to citizens (G2C), businesses (G2B), other Government agencies (G2G). E-Government has vast potential to improve and advance these interactions. It has been compared to an "endless wire" or a new method of "threading together" citizens, business and Governments within a nation [3].

E-Government functions can be classified according to “Gartner’s four phases of e-Government model” [4] which explains the progressive development of e-Government using a four-phase stage concept: (1) Presence; (2) Interaction; (3) Integration and (4) Interactive democracy. Accenture Consultancy suggests a gradual adoption that e-Government must follow to improve customer experience and thus create value: Awareness → Familiarity → Interest → Use → Satisfaction → Advocacy [5].

It is hard to establish a firm connection between ICT innovations and actual outcomes [3]. A suitable and systematic appraisal framework should include the appraisal of the e-Government system quality, the appraisal of how well a system meets user needs and the appraisal of the effectiveness of the e-Government project and its impact [6].

Researchers [7] have provided insights on measuring the overall project success of e-Government. Worldwide organizations are also constantly measuring e-Government success. Accenture focuses on best practices for customer service [8], the UN evaluates e-Government Readiness [2], and Waseda University (Japan) [9] provides an Asian perspective to assess the global development of e-Government. Leading e-Government countries are customer oriented [6] and are more and more using an interactive approach so that both government and citizens may reach a win-win situation [9].

This paper presents a strong argument that correlates the challenges and needs for successful e-Government implementation identified by the UN 2008 e-Government Readiness Survey [2]. Those are highlighted in Table 2.1.

Table 2.1 shows challenges and needs for successful e-Government implementation

E-Government Challenges and Needs (UN 2008 e-Government Readiness Survey)	
Citizen Friendly Portal Ease of Use Customer Relationship Management (CRM) Trust of the consumer Confidentiality Data Security Verification and Validation Access to Information	24/7 Accessibility One – Stop Shop Participatory Process Online Forms and Permits Shared Services Business opportunities Level Playing Field Integrated Office Operations Infrastructure

Privacy, the interest that individuals have in sustaining a personal space, becomes more important as countries move towards maturity in e-Government implementation, and the focus is on the customer.

Information privacy refers to the claims of individuals that data about themselves should generally not be available to other individuals or organizations, and that, where data is possessed by another party, the individual must be able to exercise a substantial degree of control over that data and its use [10].

The privacy impact assessment (PIA) is “an assessment of any actual or potential effects that an activity or proposal may have on individual privacy and the ways in which any adverse effects may be mitigated” [11]. To encompass the potentially harmful effects of surveillance on a wider basis than that of protecting privacy, surveillance impact assessments (SIA) have also been proposed [12].

The Organization for Economic Co-operation and Development (OECD), in 1980, detailed the fair information practices: collection limitation; purpose specification; security; accountability; individual participation; openness; use limitation and data quality [12]. Throughout the world, the privacy of information about individuals is guided by these principles, which represent basic guidelines for responsible information practices. They form the foundation of many national and local privacy laws, international agreements on data protection, and various industry codes of best practices.

The Platform for Privacy Preferences (P3P) is a protocol developed by the World Wide Web Consortium (W3C) allowing websites to declare their intended use of information they collect about browsing users. P3P gives users more control of their personal information when browsing and a more precise control of the kind of information they allow to be released.

The main content of a privacy policy includes the following: which kind of information is collected (identified or not); which information the server stores; which particular information is collected (IP number, email address, name, etc.); use of the collected information, how this information is used (for regular navigation, tracking, personalization, telemarketing, etc.); who will receive this information (only the current company, third party, etc.); permanence and visibility, how long information is stored; and whether and how the user can access the stored information (read-only, opt in, opt out) [13].

Users may not understand how integrated information and customization impact their privacy. Encryption, anonymous web-browsing, filtering devices, smart agents, privacy preference tools and the like may act as empowering instruments for the individual [14]. Users are not necessarily familiar with much of the terminology used by privacy

experts. Summary information may combine information about multiple aspects of privacy to help users understand the information being conveyed to them or allow them to make configuration decisions more easily [13].

Encryption hides what is being said, anonymity hides who is saying it and to whom [15]. Authentication and confidentiality are two security dimensions that are directly related to privacy; anonymity, access control and encryption are the key concepts for preserving privacy. Anonymous communications are a key component of Privacy Enhancing Technologies (PETs) such as TOR - a network of virtual tunnels that allows people and groups to improve their privacy and security on the Internet [16].

Building trust has been a major aim of e-Government implementation. Trust refers to Governments' true understanding of citizens' needs and the value they can deliver to citizens. Trust refers to confidence that citizens have that Government will respect their privacy concerns and handle their personal sensitive information responsibly [3]. Trust is earned over time and it is an aggregation of many peoples' experiences [1].

A consumer-centric and trust-based approach to the technology offers the greatest potential for Governments to take advantage of the revolutionary technologies that are available. Privacy can become less of an obstacle to beat and more of an opportunity for businesses to differentiate themselves, increase their financial value and even energize entire economies [17].

Government's practices in collecting, retaining, and managing a wide range of personal data about its citizens such as health records, tax returns, law enforcement records and others pose a wide range of privacy concerns [11]. Where we live, who we are and what we purchase will determine how quickly we are served and what we are offered [12].

Technologies are more intrusive today, and they will only become more so. Because the commercial value of personal data has been recognized, companies now have considerable financial incentives to take the time to gather information and to use data-mining techniques that can make inferences about customer preferences based on their private information [17].

3. Proposed models

In this paper we examine privacy as an aspect of information security. If citizens have better control over their privacy preferences, the trust level can be

increased. Figure 3.1 shows the rationale behind this approach, which consists of three independent blocks: (i) e-Government measurement models adding privacy as a major evaluation criterion; (ii) user interface that facilitates the control over privacy preferences and (iii) appropriate selection of security technologies. These three integrated blocks provide the potential and the opportunity to enhance the trust among e-Government stakeholders.

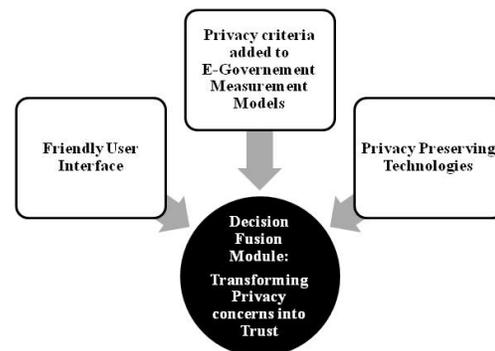


Figure 3.1 The foundation blocks for a model of preserving privacy

Currently privacy is not a major evaluation criterion of e-Government appraisal models. Adding it to current models would result in a more suitable one that generates the potential of e-Governments to earn citizens' trust, which is a major aim of leading countries in providing a customer-centric initiative. By building trust from the top of the value chain, e-Government models can lead the process of a trustworthy value chain. If trust has been created, Governments could benefit enormously from citizen users of electronic services.

We suggest a new measurement model that enforces privacy as a major criterion. It integrates the fair information principles with current e-Government evaluation models. E-Government measurement models currently do not take privacy and security as major criteria of evaluation. Apart from increased measurement accuracy, the proposed model has the capacity to motivate Governments to manage and control e-privacy more effectively. How privacy of individuals is dealt with should be a key point for the success of any e-Government project.

Based on the Fair Information Principles, the four dimensions by which e-Government should be measured in relation to privacy are: (i) data collection (collection limitation, privacy preferences, purpose specification, minimal requirement, audit training, monitoring and choice (opt in, opt out)); (ii) data transmission (encryption, security, pseudonymity); (iii) data storage (exposure and sensitivity, access controls, privacy preferences) and (iv) data usage

(access control, use limitation, data quality and accountability). These are represented in figure 3.2.

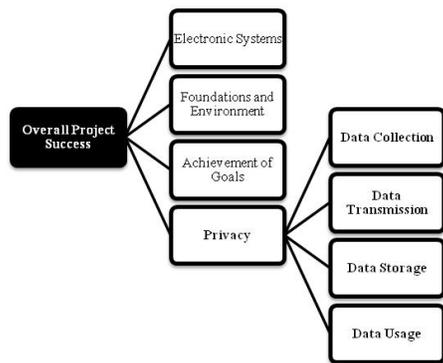


Figure 3.2 The original Appraisal Reference Model proposed by Hu, Xiao and Pang [7] in 2005 and the new suggested privacy dimensions.

The model suggested is based on the Appraisal Reference Model proposed by Hu, Xiao and Pang [7] in 2005. This appraisal framework does not put privacy and security as major evaluating criteria. So it cannot measure whether a certain e-Government project is successful or not. It is suggested that a measurement appraisal framework that incorporates user privacy as a major evaluation criteria for e-Government models would motivate e-Government to address privacy solutions more thoroughly. Additionally such criteria would represent a more accurate and precise evaluation model for e-Government performance

Specific measures should be taken by e-Government models to enforce privacy in each of the underlying privacy vulnerabilities. By proposing a new measurement model in which evaluation of privacy is addressed in these four dimensions, e-Government models will better address privacy concerns of citizens.

There is a strong need to give more control to the user of e-Government services. The authors' suggest the foundations of this user interface that facilitates user choice and enforces privacy preferences.

The suggested user interface components allow citizens to transact pseudonymously with Government, and facilitate citizens' preferences to be set. The user interface would make it possible for the user to establish the required level of privacy enforcements, such as encryption and authentication, the anonymity degree required and the level of trust the user has in the determined agency.

The interface should facilitate user interaction with the system by appropriately taking the level of anonymity required to deal with each service along with the level of trust of each agency. For each interaction, users could be able to change their

preferences and deal with the Government agency accordingly.

The user does not need to know what is happening behind the scenes as long as appropriate technical measures are in place. The user interface allows citizens to disclose personal information only needed by the specified application. Yet the more information given, more services may be provided.

The user interface would make it possible for the user to establish the required level of privacy enforcements such as encryption and authentication, the pseudonymity degree required and the level of trust the user has in the particular agency. It should also provide better information to users, with the potential to increase transparency associated with privacy practices.

4. Analysis

Privacy protection laws vary a lot in the world and general conclusions are not reliable. However, we claim that once privacy criteria are added as a major evaluation aspect of measuring e-Government success, it would force different countries into better practices of data handling.

Developing public confidence in the technology and trust framework is part of the e-Government strategy. In Australia, Gatekeeper establishes a trust framework that includes processes for identifying participants and issuing encryption keys and digital signatures. Users should have the choice of using privacy protection technologies available when dealing with Government agencies electronically.

The Australian Government controversial health and welfare Access Card was halted because it represented a threat to privacy. The Taskforce Privacy Group found inadequate constraints to prevent it becoming an ID card. Also, the supporting database could be used for unintended purposes, or linked with other databases to compile extensive information on individuals.

Next, the authors' examine the suggested new e-Government measurement model in relation to the privacy vulnerabilities identified and compare it with the overall Australian's e-Government strategy and the proposed Access Card implementation:

Data Collection: Registration for the access card is a key issue. Great care will need to be taken to specify the exact purposes for which the access card is to be introduced, but equally to specify the purposes for which it cannot be used to avoid function creep. Only the necessary data should be collected and an independent audit trail should be conducted to ensure independence and reliability in

the system. Educating users in how to preserve the private key will also be significant. Sooner or later every citizen will need to have one card to access the system, and become a person registered in the Secure Customer Registration Service (SCRS).

Data Transmission: There must be a healthy balance between privacy and security. Anonymity is feasible under the Gatekeeper Framework. Privacy and security represents a longer way to data flow, in this case, more routers and gateways could be used to avoid traffic monitoring, meaning that there might be some delay in the communication. Users must beware of these drawbacks when using these mechanisms.

Data Storage: The Government has ruled out the incorporation and use of particular biometric identifiers such as finger prints and retinal scans on the card, but will incorporate a photograph and digital signature. The technology chosen should be sufficiently user-friendly. Also, increasing the factors of authentication requires users to provide more information for the system, therefore increasing Information Security but impacting privacy. Although SCRS will be established separately from the databases administered by participating agencies, rules must be established to address data-matching expansion. The Taskforce has identified a number of privacy issues relating to SCRS.

Data Usage: There is a need to make clear a variety of matters such as: the permitted or prohibited uses of the access card and associated penalties (i.e data misuse recovery); the rules for who is authorized to access (identity management) and how access is provided to the card and stored data; and the penalties for improper behaviour related to the access card. Sensitive agency specific information will not be shared between participating agencies. The participating agencies themselves, while having access to the information in the SCRS, must maintain their own databases related to the individual entitlements of each card holder separately. Given the potentially damaging consequences of privacy invasion, transparency and accountability are important factors. Australian Privacy Policies and Regulations are the same for both offline and online contexts. Accountability has a key role here.

Users should be able to define privacy preferences, levels of trust and degree of pseudonymity required for each service provided by e-Government. The DFM takes the entered preferences and then selects appropriate mechanisms to enforce privacy. The privacy preserving user interface should enforce privacy without the need for users to understand the principles of Public Key

Infrastructure (PKI), information security or anonymity principles.

The DFM Technical Algorithms will take user inputs (levels of pseudonymity, privacy and trust), process the intake and determine the appropriate paths to follow, and would be responsible for further fine tuning, as illustrated in figure 4.1.

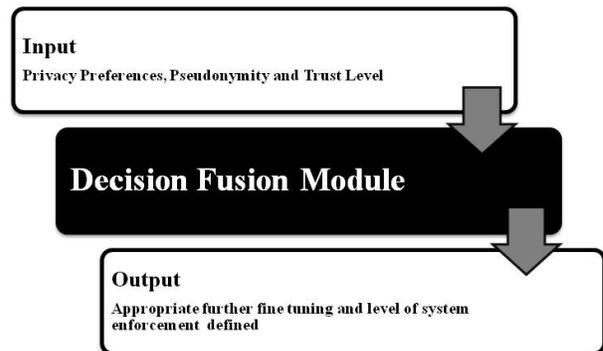


Figure 4.1. The Decision Fusion Module (DFM) process

Two scenarios are given below to facilitate comprehension and to show that gradually the system can remove or add privacy and anonymity tools as required by the user in the privacy preferences module user interface. Figure 4.2 summarizes how the DFM Algorithms works.

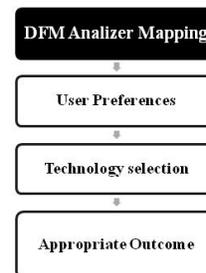


Figure 4.2. The DFM Analyzer mapping

In scenario A, the user has chosen 100% system enforcement, with very high level of privacy protection and anonymity required, and no trust at all in the agency. In this case, the model should provide the best tools available to protect anonymity (eg. Advanced Encryption Standard (AES) will be applied in the hash function, pseudonymity through TOR networks, with a higher number of routers and gateways, and access controls through a trusted third party such as identity managers.

In scenario B, the user has chosen 70% system enforcement, with high level of privacy protection and anonymity required and low trust in the agency. Instead of AES encryption, the algorithm could employ 3DES - Triple Data Encryption Standard

Algorithm - an encryption algorithm with lower strength than AES). The anonymity tool could be used through fewer routers and gateways, therefore accelerating the communication a little bit.

5. Conclusions

Technology may be either privacy-enhancing or privacy-threatening. Similarly, it may be customer friendly or unfriendly. Hence, people can use these technologies for the good and for the bad. Besides the benefits provided by e-Government, there is a range of privacy and security issues which mature e-Governments currently face. The Australian model is one such model being used to deal with these issues.

Governments and organizations must set the rules and enforce privacy policies in systems that handle citizens' personal information and maintain a healthy balance of information security and privacy. It is worth noticing that big IT players such as Google, clamour for better and more detailed privacy regulations.

The suggested user interface module could serve as the foundation for further development in preserving e-privacy, hence contributing to build trust among e-Government stakeholders. This paper has the capacity to facilitate privacy protection and enforcements in e-Government models. Again, building trust is a key concept in mature e-Government countries that are moving towards a customer-centric value creation.

E-Government evaluation models should give serious consideration to how effectively privacy concerns are addressed. An effective measurement for the initiatives of e-Government models to protect citizens' privacy would stimulate privacy enforcements throughout the whole value chain, thus building trust. The issues raised by the Taskforce regarding the Access Card provide evidence of privacy and security concerns of citizens. A user friendly interface also plays a key role in providing control for privacy preferences over personal sensitive information to citizens.

The e-Government measurement model was evaluated against the Access Card Case Study; however, it could also be applied to one existing e-Government Ranking and therefore one more accurate analysis (because it takes privacy into account) of the e-Government models of each country could be derived. The suggested user interface concept also needs to be developed further, with an accurate mapping of the interface and what each selected preference would technologically

imply. An efficient algorithm to be used by the DFM with a user friendly interface capable of giving users a higher degree of control over their privacy preference also will enhance the model.

References

- [1] A. E. Fano, S. Mathur, and B. Shah, "The economic value of trust," *Outlook 2003, Accenture*, 2003.
- [2] S. Hafeez, "UN E-Government Survey 2008 - From E-Government to Connected Government," 2008.
- [3] P. T. Jaeger, "The endless wire: E-Government as global phenomenon," *Government Information Quarterly*, vol. 20, pp. 323-331, 2003.
- [4] K. Stoltzfus, "Motivations for Implementing E-Government: An Investigation of the Global Phenomenon," *Communications of the ACM*, pp. 333-338, 2005.
- [5] C. E. Koh, V. R. Prybutok, S. Ryan et al., "The importance of strategic readiness in an emerging e-Government environment," *Business Process Management Journal*, vol. 12, no. 1, pp. 22-33, 2006.
- [6] F. B. a. J. S. Hiller, "A framework for e-Government: privacy implications," *Business Process Management Journal*, vol. 12, pp. 48-60, 2006.
- [7] Y. Hu, J. Xiao, J. Pang et al., "A Research on the Appraisal Framework of e-Government Project Success," *ICEC'05*, 2005.
- [8] Accenture, "Leadership in Customer Service: Delivering on the Promise," 2007
- [9] P. T. Obi, "Waseda University e-Government Ranking 2009", 2009.
- [10] B. N. Meeks, "The Privacy Hoax," *Communications of the ACM*, vol. 42, no. 2, pp. 17 - 19, February, 1999.
- [11] P. Anderson, and J. Dempsey, "Privacy and E-Government: Privacy Impact Assessments and Privacy Commissioners – Two Mechanisms for Protecting Privacy to Promote Citizen Trust Online," *Global Internet Policy Initiative*, May, 2003.
- [12] K. Ball, and D. M. Wood, "A Report on the Surveillance Society," *UK's Information Commissioner's Office*, 2006.
- [13] L. F. Cranor, P. Guduru, and M. Arjula, "User Interfaces for Privacy Agents," *ACM Transactions on Computer-Human Interaction*, vol. 13, no. 2, pp. 135-178, June, 2006.
- [14] R. Clarke, "Internet privacy concerns confirm the case for intervention," *Communications of the ACM*, vol. 42, no. 2, pp. 60 - 68, February, 1999.
- [15] A. Jones, "Anonymous Communication on the Internet," *Rose-Hulman Institute of Technology Conference*, Terre Haute, Indiana, USA, September, 2004.
- [16] H. Federrath, "Privacy Enhanced Technologies: Methods – Markets – Misuse," *2nd International Conference on Trust, Privacy, and security in Digital Business (TrustBus '05)*, 2005.
- [17] Accenture, "The future of identity: Biometrics solutions to enhance the performance of businesses and governments," 2005.