Association for Information Systems
AIS Electronic Library (AISeL)

CONF-IRM 2016 Proceedings

International Conference on Information Resources Management (CONF-IRM)

2016

Addressing trust, security and privacy concerns in e-government integration, interoperability and information sharing through policy: a case of South Africa

More Ickson Manda
University of the Witwatersrand, moreikson@gmail.com

Judy Backhouse
University of the Witwatersrand, judy.backhouse@wits.ac.za

10. Addressing trust, security and privacy concerns in e-government integration, interoperability and information sharing through policy: a case of South Africa

More Ickson Manda
University of the Witwatersrand
moreikson@gmail.com

Judy Backhouse
University of the Witwatersrand
Judy.backhouse @wits.ac.za

Abstract

Technology enabled government promises to deliver better services and hence facilitate better lives for citizens. However such e-government cannot be implemented without trust between government and citizens and between government departments. Concerns over information security and privacy have become a contentious issue for governments and stand in the way of that trust. Policy and legislation are two mechanisms that governments have to implement to address these concerns. The purpose of this study was therefore to identify and review policy and legislative measures implemented by the South African government to address information security and privacy as well as e-government information sharing, integration and interoperability. The study is an interpretive case study using documentary evidence and a review of literature as data collection methods. The study found that South Africa has implemented a number of policy and legislative measures aimed at addressing these concerns. The study concluded that some of these measures are compromised by poor implementation, poor coordination in government, poor state of governance, conflicting legislation and policy and poor compliance.

Keywords

Integration, interoperability, trust, privacy, security, e-government, institutional theory

1 Introduction

Governments are under immense pressure from stakeholders to deliver services so as to improve the lives of citizens. E-government interoperability, integration and information sharing is one of the key strategies governments worldwide are implementing to improve synergies across government agencies and increase efficiency in service delivery (Pardo, Nam & Burke, 2011).Trust, security and privacy concerns have however been identified as major barriers to successful e-government integration, interoperability and information sharing (Yang & Maxwell 2011; Lips, O'Neill & Appel, 2011; Fan, Zhang & Yen, 2014). Technology advances in e-government make it increasingly challenging to control privacy-intrusive applications (Acquilina, 2010). Privacy and security are key elements in building citizens' trust in e-government services (Alawneh, Al-Refai & Batiha, 2013). Concerns over citizens' privacy in the digital and connected environment are a major threat to the success of e-government initiatives due to increased scepticism and mistrust of e-government initiatives by citizens because of the concern over invasion of citizen privacy (Belanger & Hiller, 2006). In South Africa, interoperability and security have been identified as two of the five the pillars for successful e-government. The 2001 e-government policy framework however stresses that "interoperability should be achieved without compromising vital IT security concerns" (Department of Public Services and Administration, 2001).

This study focuses on organisational, semantic and policy interoperability as the goal is to understand non-technical issues such as policy, trust, privacy and culture in e-government interoperability. Organisational interoperability focuses on collaboration and alignment of processes to achieve shared goals. Semantic interoperability focuses on the application, meaning and interpretation of data and information being exchanged between systems. Policy interoperability focuses on compatibility between policies, laws and regulations in facilitating interoperability (Goldkuhl, 2008; Charalabidis *et al*, 2010). Technical interoperability which focuses on technical issues is excluded as this is not the focus of the study.

According to Elmaghraby and Losavio (2014), legal and social concepts of a citizen's ''right to privacy'' are intertwined with the challenge of security and the benefits of smart initiatives. Governments, including the government of South Africa, have responded to these concerns by developing policies, legislation and other mechanisms for addressing security, privacy and trust concerns in e-government. One of the biggest challenges will be to ensure coherence of these policies (Wright, Gutwirth, Friedewald, De Hert, Langheinrich & Moscibroda, 2009). The purpose of this study was therefore to identify and review legislation and policy measures implemented by the government of South Africa to strengthen information security, privacy and trust in e-government integration and interoperability.

The main **research question** shaping this study is:

> *How can policy be strengthened to address trust, security and privacy concerns in e-government integration and interoperability?*

The following are the main **objectives** of this study:

- To review the extent to which legislation and policies in South Africa address security, privacy and trust concerns in e-government.
- To identify some of the challenges compromising the effectiveness of policy and legislation in promoting privacy, security and trust in government institutions.

The paper is divided into two sections; the first section reviews literature on security, privacy and trust concerns in e-government integration, interoperability and information sharing; the second section identifies and reviews how policy and legislation in South Africa addresses privacy, security and trust concerns in e-government and identifies weaknesses in policy.

2 Methodology

The study is a qualitative interpretive case study that employs documentary evidence as its main data collection method. An extensive review of literature was conducted to assist in conceptualising the problem being investigated. The other aim of reviewing literature was to review published evidence on trust, security and privacy issues in e-government interoperability and compare with the findings of this study so as to identify and close gaps, thus adding to the e-government body of knowledge.

We analysed the national cyber security framework, government ICT corporate governance framework, proposed integrated ICT policy, minimum information security standards, minimum interoperability standards and proposed online regulation policy to ascertain the extent to which they address privacy and security and trust concerns in e-government in South Africa. Relevant legislation addressing interoperability, security and privacy is also reviewed (*see section 5.3*). Thematic analysis, was conducted using closed (deductive) coding

based on themes identified in literature and theory to identify and classify themes in the documents analysed.

3 Theoretical framing

Institutional theory is used to underpin this study. Institutional theory is a multi-disciplinary theory that is drawn from disciplines such as organisational behaviour, political science, sociology and economics (Scott, 2014). Scott (2014) defines an institution in terms of activities and resources associated with regulative, normative and cultural-cognitive mechanisms which legitimise the institution. In the case of government, legislation represents regulative measures to coerce particular behaviours, while policy represents more normative measures, defining appropriate and morally sanctioned behaviour. Trust, privacy and security in e-government interoperability and integration are complex issues which can be studied from many perspectives. This influenced the use of institutional theory which helps in understanding the interlinked and complex relationships inherent among institutional mechanisms, technology, socio-economic context and organisational factors in which they are embedded (Luna-Reyes& Gil-Garcia, 2011). The theory also helps in understanding the internal and external pressures organisations are subjected to (Bjorck, 2004; Jacobson, 2009).

Institutional theory is a theory of social behaviour and is used in this study to understand and explain human actions in institutions (Bjorck, 2004). We use institutional theory to understand and explain social behaviour affecting, security, privacy and trust in e-government interoperability. We examine institutional regulative mechanisms such as legislation used to influence social behaviour through legal sanctioning. Normative mechanisms such as policy and standards are also examined and their role in introducing a prescriptive, evaluative, and obligatory dimension into social life Scott (2014). Cultural cognitive elements in institutions which culminate in a culturally supported basis for legitimacy as described by Jacobson (2009) and Scott (2014) are also examined.

4 Literature review: Trust in e-government

Citizens' trust of government, technology and e-government initiatives has a bearing on citizens' participation in and adoption of e-government (Goldfinch, & Herbison 2009). Before endorsing e-government initiatives, citizens must believe government agencies possess the capability for successfully implementing and securing these systems. Open and corruption-free citizens' interaction with e-government service providers will enhance citizen trust and acceptance of e-government services. On the contrary, unfulfilled promises, corruption and dishonesty from government officials and employees will decrease trust and increase opposition to these initiatives (Bélanger & Carter, 2008). Distrust in government intentions often result in citizens withdrawing from voluntary compliance with governmental demands, regulations and resistance to governmental policy which prevents the government from performing effectively. Citizen participation in e-government initiatives was thus found to have a positive impact in building citizens trust in government (Kim & Lee, 2012). Gaining citizens' trust thus helps reduce complexities and helps gain efficiencies in public sector administration (Smith, 2010).

Trust issues among government agencies themselves have posed serious challenges in e-government. Studies in government-to-government information sharing and interoperability in New Zealand and China revealed that lack of trust among participating government

agencies is a constraint to information sharing and interoperability in e-government (Lips, O'Neill & Appel, 2011; Fan, Zhang & Yen, 2014).

Al-Omari and Al-Omari (2006) proposed an e-government trust model (Figure 1) and identified five building blocks of trust in e-government. These include:

- Legislation and legal cover which forms a strong basis for building trust by providing a legal framework for both the government and its customers
- Policies and procedures that support the legal framework and promote transparency in government are critical in building trust.
- Social and cultural practices such as previous experiences, equal and fair treatment of citizens and accountability by government is critical in fostering trust
- Information technology security needs to be integrated with other trust elements to foster trust in e-government
- Process automation is the last element in building e-government trust by speeding up processes and delivery channels.

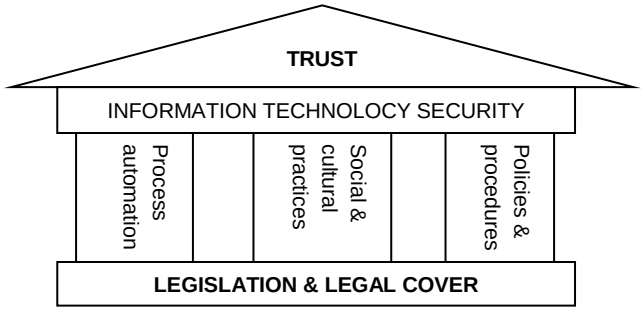

Figure 1: E-government trust model (Al-Omari & Al-Omari, 2006)

Critique of the E-government trust model

The model covers basic trust building blocks such as social and culture practices, legislation and legal cover, policy and procedures, IT security and process automation. It however falls short in incorporating other determinants of trust such as privacy controls, information sharing, governance and citizen participation.

4.1 Mistrust between government agencies

Implementing e-government requires integration, interoperability and information sharing across government agencies. These cannot be achieved without trust between government agencies, which is often lacking. Several contributing factors giving rise to this can be identified from the literature. These are listed in Table 1.

Factors	Reference
Reputation: Fear that interoperability, integration and information sharing may result in misrepresentation of information.	Yang & Maxwell 2011; Lips, O'Neill & Appel, 2011; Fan, Zhang & Yen, 2014;
Sabotage: Fear of misuse of the information resulting in the sharing agency incurring liabilities	Yang & Maxwell 2011; Lips, O'Neill & Appel, 2011; Fan, Zhang & Yen, 2014
Legal: Fear of the legal consequences of exposure to sensitive information	Fan, Zhang & Yen, 2014
Power and politics: Political risks of losing authority or source of power.	Yang & Maxwell 2011; Fan, Zhang & Yen, 2014
Economics of information: Loss of competitive advantage.	Zhang & Dawes, 2006
Quality concerns: Mistrust of the quality of information shared	Yang & Maxwell 2011
Loss of autonomy: The sharing government agency fears losing control once information is shared or when systems are integrated.	Yang & Maxwell 2011
Public scrutiny: Government agencies may feel sharing information exposes them to risks such as public scrutiny	Yang & Maxwell 2011

Table 1: Factors contributing to lack of Trust in e-government

Some of the factors highlighted in table 1 reflect cognitive-cultural assumptions, such as that "knowledge is power", which work against interoperability, integration and information-sharing, but are difficult to change.

4.2 Trust as a multidisciplinary concept

Trust is a multidimensional and complex phenomenon which has been studied from various disciplines, with each discipline focusing on distinct issues. Research into trust has taken many approaches including economic, managerial, human computer interaction, sociology and the technological approach (Colesca, 2009).

The five different approaches all provide useful lenses for understanding trust issues in e-government. This is important because of the complexity and multidimensional nature of trust (McLeod & Pippin, 2009).Tolbert and Mossberger (2006) further categorise trust into two types:

(i) **Process-based trust** is rooted in repeated interactions with government and on the perceptions, resulting from those interactions, that government is responsive. Process based trust is anchored on (a) responsiveness of government through enhancing communication with citizens, (b) increasing access to information and government services through online platforms,(c) increasing citizen participation and (d) improved efficiency and effectiveness of e-government services.

(ii) **Institution-based trust** is based on the judgment of institutions rather than interactions and it conveys an expectation that institutions will "do what's right."Institution-based trust thus refers to an individual's perceptions of the institutional environment, including the structures and regulations that make an environment feel safe (McKnight, Choudhury & Kacmar 2002). Institution-based trust is anchored on (a) transparency, (b) responsibility of government with citizens' information through policy and legislative measure, (c) increasing citizen participation and (d) improved efficiency and effectiveness of e-government services.

This means that policy and legislation contribute primarily to building institution-based trust, they do not directly improve process-based trust, although in the long term they contribute to this as responsiveness, access and efficiency improves.

4.3 Determinants of trust in e-government: privacy and security trust

4.3.1 Privacy trust

The use of ICT in interoperability, integration and information sharing in government has given rise to ethical dilemmas related to the sharing and use of personal information. Technology advances make it increasingly challenging to control the privacy-intrusive use of ICT (Acquilina, 2010). Protecting citizens' privacy has become a priority for governments in building citizen's trust in e-government initiatives (Alawneh, Al-Refai & Batiha, 2013). Concerns over citizens privacy in a digital environment is a major threat to the success of e-government initiatives due to increased scepticism and mistrust of e-government initiatives by citizens (Belanger & Hiller, 2006). Privacy trust is defined as "the belief that personal information entered into a system will remain private" (McLeod & Pippin, 2009:3).

Wright *et al* (2009) also identifies some of the challenges confronting governments in enacting policies that address privacy concerns:

- Societal challenges – different interpretations of privacy by different stakeholders due to differences in social institutions, practices and behaviour. Different interpretations also

arise due to developments and global events that transform debate about privacy in a very short time such as the September 11 terrorist attack which quickly raised counter-terrorism and national security to the top of public policy agenda.

- Technical challenges – developments in new and emerging technologies that transform ways of collecting and analysing personal information from multiple, disparate sources.
- Economic challenges - convincing industry of the importance of investing in privacy enhancing mechanisms, affordability of deployment of privacy enhancing mechanism and dealing with issues on the economics of information.
- Political challenges – achieving coherence, adequacy and the consistent application of privacy policy both in the public and private sector.

4.3.2 Security trust

The increased use of technology in e-government through online transactions between government and citizens (Government to Citizen), government and business (Government to Business) and government departments (Government to Government) has increased security concerns. Security trust is defined as "the belief that the information system will be safe from hacking and the introduction of viruses or other malware" (McLeod & Pippin, 2009:3). There is also a close relationship between trust and security in e-government. Perceived security of technology is thus an important determinant of trust in e-government (Colesca, 2009).

Increases in cyber terrorism and fraud has caught the attention of governments worldwide (Weimann, 2005). Cyberterrorism is the use of ICT tools to sabotage or shut down critical national infrastructures such as government operations, transportation and energy (Weimann, 2015). Governments have responded by enacting policies and legislation dealing with cyberterrorism threats e.g. the Cyber security Act of 2012 in USA. Developing countries such as China and South Africa are also in the process of adopting cyber security related legislation.

4.4 Promoting security, privacy and trust through policy and legislation

The formulation of policy is important in promoting trust, privacy and security through guides, procedures, compliance programmes and training (Al-Omari & Al-Omari, 2006).Wright *et al* (2009) however warns against the reliance on "broad-brush" policies which are unlikely sufficient to tackle new challenges, arguing that we are entering an era that will require development of ''micro-policies'' that address specific issues of privacy and security. Policy however is a normative institutional mechanism that establishes guidelines for appropriate actions.

Legislation is a regulative institutional mechanism and is viewed by some as the cornerstone for building trust, security and protecting citizen's privacy (Al-Omari & Al-Omari, 2006). Several measures are identified, these include the following:

- *Establishing new acts to protect the privacy and confidentiality of customers*
- *Establishing acts to solve global concerns such as the Internet*
- *Issuing new legislation to manage the Internet*
- *Creating a national information infrastructure or legal framework for online business*
- *Providing a new legal framework for digital communication and transactions.*

5 Policy discussion and analysis

South Africa, post-apartheid, has made significant progress in policy and legislative reforms aimed at protecting constitutional rights to privacy and security. However, the digital environment and the adoption of e-government brought a new dimension to concerns of security, privacy and trust in government initiatives.

South Africa has implemented various policies and legislation aimed at addressing security, privacy and trust concerns. One of the major setbacks in policy is that South Africa has not developed a new e-government strategy since the implementation of the first e-government policy framework by the Department of Public Service and Administration (DPSA) in 2001. This is a weakness in e-government strategy and policy considering fast-paced developments in technology that have an impact on e-government. The e-government policy framework (Department of Public Services and Administration, 2001), despite addressing crucial issues such as interoperability and information technology security, omitted contentious issues and new developments in e-government such as technology convergence, mobile government, privacy and trust concerns in connected and smart societies. In this section the current state of policy and legislation in South Africa is reviewed.

5.1 The South African constitution

The rights to privacy and security are enshrined in the South African constitution. **Section 14** of the South African constitution addresses privacy. It states that everyone has the right to privacy, which includes the right not to have their person or home searched; their property searched; their possessions seized; or the privacy of their communications infringed. **Section 198** address national security and stipulates that national security must reflect the resolve of South Africans, as individuals and as a nation, to live as equals, to live in peace and harmony, to be free from fear and want and to seek a better life (South Africa, 1996).

5.2 National ICT policy framework in South Africa

The following sections will discuss ICT policy with a focus on privacy and security.

5.2.1 Integrated National ICT policy framework

In response to the challenges caused by fragmentation of ICT policy and to take advantage of convergence of communication technologies, in 2013 the government of South Africa began to develop an integrated ICT policy framework. The proposed integrated ICT policy framework is set to become "government's formal policy position on key issues relating to Information and Communications Technologies (ICTs)" (Department of Telecommunications and Postal services, 2015). The policy reiterates that public and business confidence and trust in the cyberspace is critical to promote both e-government and e-commerce growth in South Africa. The policy prioritises the need to address cybercrime, data protection, privacy protection, consumer protection and protection of children as a measure to ensure trust and confidence in the cyberspace.

5.2.2 National Cyber Security Framework

In 2012, the government of South Africa developed the National Cyber Security Framework. The National Cyber SecurityAdvisory Council was subsequently established in 2013 with a mandate to advise government on cyber security policies. The establishment of the cyber securityhub as well as the national Computer Security Incident Response Team (CSIRT) is a significant milestone in strengthening cyber security in South Africa. The cyber security framework addresses some of the security concerns in a cyber environment. The aim of the framework is to:

- *Promote a cyber security culture and facilitate compliance with minimum security standards;*
- *Strengthen mechanisms and ensure adequate capacity in place to prevent and address cybercrime, cyber warfare, cyber terrorism, and other related issues;*
- *Establish public-private and societal partnerships within South Africa and internationally to strengthen awareness and enforcement;*
- *Ensure the protection of national critical information infrastructure; and*
- *Promote and ensure a comprehensive legal framework governing cyberspace* (Department of Telecommunications and Postal Services, 2015).

The National Cyber Security Policy is still to be implemented. Delays are concerning and leave South Africa vulnerable given the rise in incidents of cyberterrorism globally.

5.2.3 ICT governance in government

South Africa's first democratic government inherited a fragmented, unaccountable and racially divided governance system (The Presidency, 2014). The 2009 King III Report on governance for South Africa addresses the need for good governance of ICT and information. The King III report also addresses concerns about data privacy and information security. It mandates formal processes to manage and govern information, which encompasses information security, and personal information privacy. The incorporation of ICT into the overall risk strategy of organisations to ensure that ICT risks are adequately addressed through risk management, monitoring and assurance processes is an important development in ICT governance.

In 2012, the government of South Africa implemented the ICT corporate governance framework to institutionalise the governance of ICT as an integral part of corporate governance within government in a standardised and coordinated manner (Department of Public Service and Administration, 2012). To strengthen ICT governance in government the framework stipulates that all ICT decisions of importance should come from senior political and managerial leadership and should not be delegated to technology specialists.The management of information should be carried out on the same level as the management of other resources such as people, finance and material in the Public Service.Top leadership support and the recognition of information as an equally important resource is set to increase the prioritisation of ICT as a resource of strategic importance in government. This is important in e-government which requires top leadership commitment in driving e-government through implementation of relevant strategies, policies and other mechanisms.

Such improvements in governance within government serve to support increased institution-based trust in the sense of Tolbert and Mossberger (2006).

5.2.4 Standards: Minimum Information Security Standards (1996)

In 1996, the government implemented the Minimum Information Security Standards. These provide for the need to ensure confidentiality and integrity of the data stored electronically and systems availability. The standards are an example of balancing the democratic right to access to information and restriction of access to confidential information. Assessment of the state of security in government institutions by the National Intelligence Agency in 2007 revealed that information security was still poor due to human error, poor infrastructure and non-adherence to prescriptions (National Intelligence Agency, 2007). What is concerning is that the updated National Security regulations were drafted several years ago but these were

not published and implemented (Department of Telecommunications and Postal services, 2015). This points to weak institutional mechanisms for promoting security in e-government.

5.2.5 Standards: Minimum Interoperability Standards (MIOS)

Adherence to common standards is important in achieving interoperability and strengthening security in information systems (Dos Santos & Reinhard, 2012). The South African government adopted Minimum Interoperability Standards (MIOS) in 2008. The purpose of the MIOS is to prescribe open system standards that will ensure a minimum level of interoperability within and between ICT systems that are utilised ingovernment, in industry, by citizens and the international community, in support of thee-government objectives. Interoperability can lead to greater effectiveness and efficiency in government services, thus enabling greater institution-based trust and, in the longer term, greater process-based trust as well. Standards selected need to support a secure IT environment.What is worrying is lack of compliance in adopting the MIOS by some government institutions (Department of Telecommunications and Postal services, 2015).

5.2.6 Online regulation policy

The Online Regulation Policy aims to transform online content regulation in South Africa through digital content classification and compliance monitoring to ensure that children are protected from exposure to disturbing and harmful content (South Africa, 2015). This policy has however been seen as a government attempt to censor the internet. The policy could be interpreted as a reduction in transparency, reducing trust in government.

5.3 Legislation: Privacy and security protection in South Africa

Legislation is a regulative institutional measure that serves to enforce policy and ensure compliance. Key legislation that addresses privacy and security in e-government are discussed briefly below.

- **The Protection of Personal Information (POPI) Act, 2013** proposes several ways in which privacy; security and trust concerns should be addressed by promoting transparency with regard to what information is collected and processed, including the capturing of data, ensuring accuracy and removing data that is no longer required. The Act also addresses issues related to quality of information (section 16), security measures on the integrity and confidentiality of personal information (section 19) and the right of the data subject to access their personal information held by another party (section 23).
- **The Electronic Communication and Transactions Act, 2002** regulates the collection, use and protection of personal information obtained through electronic transactions. Section 51 of the Act outlines the principles for collecting personal information electronically. The Act promotes privacy and security by governing the requirements and restrictions on the collection, use, storage and disposal of personal information.
- **The Regulation of Interception of Communications and Provision of Communication-Related Information Act, no 70 of 2002** regulates the interception of certain communications. This Act has been criticised for infringing people's constitutional right to privacy as stipulated in section 14 of the South African constitution. The argument for the provisions of the Act is that they are necessary for national security. The right to privacy like any other right is not absolute. The Act is thus an example of an attempt to balance between the people's rights to privacy and national security.
- **The Public Service Act, 1994** places the responsibility of governance and the management of e-government and ICT with the Minister of Public Service and Administration e.g. the Ministry developed the first e-government policy framework in 2001 and the public service ICT corporate governance framework in 2012.

- **The State Information Technology Agency (SITA) Act, no 88 of 1998** gives the State Information Technology Agency (SITA) a mandate to consolidate and coordinate the State's information technology resources in order to achieve cost savings through scale, increasing delivery capabilities and enhancing interoperability. SITA is responsible for implementing the Interoperability Standards for improving e-government interoperability.
- **The Consumer Protection Act, no 68 of 2008** sets out an overarching framework for consumer protection in South Africa including citizens 'rights to privacy.
- **Cybercrimes and Cybersecurity bill, 2015** seeks to create offences and impose penalties which have a bearing on cybercrime; to further regulate jurisdiction of the courts and protect critical national information infrastructure and further regulate aspects of international cooperation in respect of the investigation of cybercrime. Cybercrime is estimated to be costing South Africa 5.8 billion Rands (ENCA news, 2015).

5.4 Weaknesses in current policy and legislation

Policy and legislation are useful, but not infallible institutional mechanisms. Here we identify some of the forces that have compromised the effectiveness of policy and legislation in building trust and addressing security, privacy and interoperability, integration and information-sharing in e-government.

To start with, South Africa hasn't updated its e-government strategy framework which was implemented in 2001. With the fast paced developments in e-government and technology, the strategy is now outdated and falls short in adequately addressing security, privacy and other technological developments.Updating of standards has also been poor. Standards such as the Minimum Information Security Standards (1996) and Minimum Interoperability Standards haven't been updated. This is concerning given technology developments which render the application of such standards impractical. Not keeping policy elements up to date may reflect a lack of resources in the institution, or it may be that the activities (of making these updates) are not being emphasised or supported within the institution.

Non-compliance to standards by government agencies as reported in the integrated ICT policy discussion paper (Department of Telecommunication and Postal services, 2015) is also worrying. Evidently the presence of regulative mechanisms such as rules and standards is not sufficient to influence positive development in e-government if they are not enforced.

South Africa has made significant progress in establishing legislation that addresses issues of privacy and security. One of the greatest concerns is poor and slow implementation of the legislation. The Cyber Crimes and Cyber Security bill is still in draft and hasn't been promulgated. This leaves the South African cyberspace vulnerable to attack. The POPI Act which came into law in 2013 is still to be fully implemented. Such delays will result in continued non-compliance and disregard of privacy protection measures. Again, these delays point to institutional weaknesses in resourcing and the activities which are being prioritised.

Compliance has also been poor, the Electronic Communication and Transactions Act, 2002 for example called for the development of the integrated e-strategy by the government, something which the government has failed to do to date. Legislation is therefore not adequate if there is non-compliance. Failure to achieve institutional goals through legal sanctioning suggests that regulative mechanisms are not sufficient in shaping institutional behaviour. Institutional behaviour is thus also morally governed through normative mechanisms such as the social obligation to uphold high ethical standards in e-government. In the absence of perceived ethical standards, mistrust increases. Mistrust of the government

policy position in the draft Online Regulation policy (2015) is a good example, the Library and Information Association of South Africa, commenting on the draft policy on the 7th of April 2015, rejected it claiming that it infringes on the constitutional rights to freedom of access and communication and constitutes an attempt by government to censor the internet.

Slow update of legislation is a major concern in South Africa. A significant example is the amendment Bill of the Electronic Communication and Transaction Act which was drafted in 2012 and is still yet to be finalised. This has created a risk of poor harmonisation with newer laws and policies such as the POPI Act and cybercrime and cyber security policies. Urgent update and amendment of legislation is critical to avoid potential conflict with newer laws and policies. Thus we see that the legislative and policy frameworks are not as effective as they could be, limited as they are by institutional resources and activities.

6 Conclusion

In efforts to deliver a better quality of life to all citizens, the South African government is moving towards greater use of e-government. For e-government to work requires trust, but trust is impacted by security and privacy concerns. E-government also requires interoperability, integration and information-sharing between government agencies and for this it is necessary for these agencies to trust each other. The South African government is under pressure from various stakeholders to adopt and implement privacy and security measures so as to build confidence and trust. The enacting of policy and legislation represent appropriate regulative and normative institutional measures to address these issues. Policy paves the way for the implementation of legislation.

South Africa has made headway in building trust in e-government though upholding the constitutional rights to privacy and security by enacting relevant policy and legislation. Slow implementation of policies emerged as one of the major setbacks in addressingthese issues. From an institutional theory perspective we conclude that both regulative and normative institutional mechanisms are needed, and perhaps also cultural-cognitive changes, to shape social behaviour. In addition, institutions need resources and to engage in appropriate activities. Policy implementation has been compromised by these elements in the government institution, often leading to good policies being labelled as failures.

Future studies should also focus on examining how non-regulative institutional mechanisms can enhance e-government integration and interoperability. Research into ways in which a balance between regulative and non-regulative institutional mechanism can be achieved to enhance e-government integration and interoperability also deserve closer attention in e-government research.

References

Alawneh, A., Al-Refai, H. and Batiha, K. (2013) “Measuring user satisfaction from e-Government services: Lessons from Jordan”. Government Information Quarterly, 30(3), 277-288.

Al-Omari, H. and Al-Omari, A. (2006) “Building an e-Government e-trust infrastructure”, AmericanJournal of Applied Sciences, 3(11), pp. 2122-2130.

Aquilina, K. (2010) “Public security versus privacy in technology law: A balancing act?” Computer Law & Security Review, 26(2), pp.130-143.

Bélanger, F. and Carter, L. (2008) “Trust and risk in e-government adoption”, The Journal of Strategic Information Systems, 17(2), pp. 165-176.

Belanger, F. and Hiller, J. S (2006) “A framework for e-government: privacy implications”, Business process management Journal, 12(1),pp. 48-60

Bjorck, F. (2004) “Institutional theory: A new perspective for research into IS/IT security in organisations”. Proceedings of the 37th Hawaii International Conference on System Sciences.

Charalabidis, Y., Lampathaki, F., Kavalaki, A. and Askounis, D (2010) “A review of interoperability frameworks: patterns and challenges”. International Journal of Electronic Governance, 3 (2), 189–221.

Colesca, S. E. (2009) “Understanding trust in e-government”, Engineering Economics, 63(4), pp.1-9.

Department of Public Services and Administration (2001) “Electronic Government: the digital future a public service it policy framework”. [Online] Available from: http://www.dpsa.gov.za/ [Accessed: 12/10/2015]

Department of Public Services and Administration (2012) “Public service corporate governance of information and communication technology policy framework”. [Online] Available from: http://www.gov.za/sites/www.gov.za/files/CGICTPolicyFramework.pdf [Accessed: 10/10/2015]

Department of Telecommunications and Postal Services (2015) “Integrated ICT policy discussion paper”.[Online] Available from: www.dtps.gov.za [Accessed: 05/09/2015]

Dos Santos, E.M. and Reinhard, N (2012)“Electronic government interoperability: Identifying the barriers for frameworks adoption”, Social Science Computer Review, 30(1), pp. 71-82.

Elmaghraby, A. S. and Losavio, M (2014) "Cyber Security Challenges in Smart Cities: Safety, Security and Privacy," Journal of Advanced Research, 5(4), pp. 491-497.

ENCA News (2015) “Cyber hacking, a costly affair”. [Online] Available from: https://www.enca.com/life/cyber-hacking-costly-affair [Accessed: 10/11/2015]

Fan, J., Zhang, P. and Yen, D. C (2014) “G2G information sharing among government agencies”, Information & Management, 51(1), pp. 120-128.

Goldfinch, S., Gauld, R. and Herbison, P. (2009) "The Participation Divide? Political Participation, Trust in Government, and E-government in Australia and New Zealand", Australian Journal of Public Administration, 68(3), pp. 333-350.

Goldkuhl, G (2008) "The challenges of Interoperability in E-government: Towards a conceptual refinement". In Proceedings pre-ICIS 2008 SIG government Workshop.

Jacobson, D (2009) "Revisiting IT governance in the light of institutional theory".Proceedings of the 42nd Hawaii International Conference on System Sciences.

Kim, S. and Lee, J (2012) "E-Participation, Transparency, and Trust in Local Government", Public Administration Review, 72(6), pp. 819-828.

Lips, A.M., O'Neill, R. and Eppel, E.A (2011) "Cross-agency collaboration in New Zealand: an empirical study of information sharing practices, enablers and barriers in managing for shared social outcomes", International Journal of Public Administration, 34(4), pp.255-266.

Library and Information Science Association of South Africa (2015) LIASA's Statement on the FPB Draft Online Regulation Policy.[Online: Available from: http://www.liasa.org.za/node/1448. [Accessed: 12/10/2015]

Luna-Reyes, L. F. and Gil-García, J. R (2011) Using institutional theory and dynamic simulation to understand complex e-Government phenomena. Government Information Quarterly, 28(3), 329-345.

McLeod, A. J.and Pippin, S. E (2009) "Security and privacy trust in e-government: Understanding system and relationship trust antecedents". In System Sciences, 2009. HICSS'09. 42nd Hawaii International Conference on (pp. 1-10). IEEE.

National Intelligence Agency. (2007) Minimum Information Security Standards. [Online] Available from: http://www.dpsa.gov.za/dpsa2g/documents/ [Accessed: 12/10/2015]

Pardo, T. A., Nam, T., and Burke, G. B. (2011) "E-government interoperability: Interaction of policy, management, and technology dimensions. Social Science Computer Review, 30(1), pp 7-23.

Scott, W. R. (2014) Institutions and organizations. Thousand Oaks, CA, Sage

Smith, M. L (2010) "Building institutional trust through e-government trustworthiness cues", Information Technology & People, 23(3),pp. 222-246

South Africa (1996) Constitution of the republic of South Africa, Government Gazette, 108 (1996).

South Africa (2015) Draft online regulation policy, Government Gazette, 578 (38531):1-36.

The Presidency (2014) "Twenty year review: South Africa 1994 – 2014". [Online] Available from: www.thepresidencydpme.gov.za [Accessed: 12/01/2015]

Tolbert, C.J. and Mossberger, K (2006) “The effects of e-government on trust and confidence in government”, Public Administration Review, 66(3), pp.354-369.

Weimann, G (2005) “Cyberterorism: The sum of all fears?”, Conflict & Terrorism, 28(2), pp.129-149.

Yang, T. M. and Maxwell, T. A. (2011) “Information-sharing in public organizations: a literature review of interpersonal, intra-organizational and inter-organizational success factors”, Government Information Quarterly, 28(2), pp. 164-175.

Zhang, J. and Dawes, S. S. (2006) “Expectations and perceptions of benefits, barriers, and success in public sector knowledge networks”, Public Performance & Management Review, 29(4),.pp. 433−466.