

"PARANOID" OR JUSTIFIED: E-GOVERNMENT AND PRIVACY

Maria Farelo

Assignment submitted in partial fulfillment of the requirements for the degree of MPhil
in Information and Knowledge Management at the
University of Stellenbosch

Supervisor: Prof. B. Fouche

April 2004

DECLARATION

I, the undersigned, hereby declare that the work contained in this Research Assignment is my own original work and I have not previously in its entirety or in part submitted it at any university for a degree.

ABSTRACT

Electronic government holds the promises of enabling government to become more efficient in the delivery of services to the public. E-government would ultimately mean that government departments would not work in isolation from each other. The electronic environment would mean that databases would be linked and that information would be shared across all levels of government.

There are a number of issues that are presently, and will increasingly in the future impact on the success of e-government. The paradox for e-government is that while this sharing of information, paints a picture of an ideal state of affairs, that would benefit both citizen and state, there could be enormous effects on privacy. These are the ability for government to compile comprehensive profiles on citizens without their knowledge or consent. Another impact on privacy is that wrong information can be linked to the wrong person thereby impacting on the identity of an individual. Data protection and record management policies and legislation are necessary to protect personal data and information.

EKSERP

Elektroniese regeringsdienste hou enorme voordele in om 'n meer effektiewe diens aan 'n land se inwoners te lewer. 'n E-regering stel staatsdepartemente in staat om nie meer in isolasie te werk nie, dat databasisse gekoppel en inligting op alle regeringsvlakke gedeel kan word.

Daar is egter elemente in 'n e-regeringstruktuur wat 'n beduidende impak op die toekomstige sukses daarvan kan uitoefen. Die paradoks van 'n e-regering is dat hoewel dit 'n ideale prentjie skilder, dit 'n enorme impak op die privaatheid van beide die inwoners en die regering van 'n land kan uitoefen. Dit voorsien 'n geleentheid waar die regering 'n uitgebreide persoonsprofiel kan saamstel, sonder die medewete of toestemming van die persoon. 'n Verdere aspek is dat die inligting aan die verkeerde persoon gekoppel kan word, wat 'n negatiewe impak op die identiteit van so 'n persoon kan hê. Dit op sigself maak data- en dokumentbeheer, beleide and wetgewing 'n noodsaaklikheid voorvereiste vir die beskerming van persoonlike data en inligting.

ACKNOWLEDGEMENTS

I would like to thank all of the people who have supported me during the arduous process of writing this dissertation.

I would like to sincerely thank Professor Ben Fouche and Dr Martin van der Walt for their continuing faith in my ability to master the academic world. I would like to thank fellow students who have assisted me through long distance discussion and the sharing of information. My gratitude also goes to the Presidency who has allowed me the time and space to do the work.

And last but not least, I would like to thank all my friends and family who have been waiting for me to join the land of the living once more

CONTENTS**CHAPTER 1****BACKGROUND, PROBLEM STATEMENT AND OBJECTIVES OF THIS RESEARCH**

1.1 Background	8
1.2 Problem Statement	9
1.3 Objectives of this Research	12
1.4 Limitations of this Research	12
1.5 Research Design and Methodology	12
1.6 Outline of Chapters	14

CHAPTER 2**E-GOVERNMENT**

2.1 Introduction	16
2.2 Defining e-government	17
2.3 Activities and Principles	19
2.4 Barriers and Constraints	22
2.4.1 Cooperation between Departments	22
2.5 E-government paradox	23
2.5.1 The South African situation	24
2.6 Conclusion	25

CHAPTER 3**PRIVACY**

3.1 Introduction	26
3.2 Defining Privacy	27
3.2.1 Information Privacy	28
3.2.2 Communications Privacy	28
3.2.3 Territorial Privacy	29
3.3 Privacy in the South African context	30

3.4 Information for Government	31
3.5 Conclusion	33

CHAPTER 4

PRIVACY AND DATA MANAGEMENT

4.1 Introduction	34
4.2 Data Management	35
4.2.1 What is Data Management?	36
4.3 Data Protection	38
4.3.1 What is Data Protection?	39
4.4 Data Security	39
4.4.1 Digital Signatures	40
4.5 South African efforts at Data Management	41
4.5 Policy and legislative measures	41
4.6 Conclusion	44

CHAPTER 5

RECOMMENDATIONS AND CONCLUSION

5.1 Introduction	46
5.2 Summary of Literature	46
5.2.1 E-government	46
5.2.2 Privacy	46
5.2.3 Privacy and Data Management	47
5.3 Recommendations	47
5.4 Areas for further research	48
5.5 Conclusion	49

REFERENCES	50
-------------------	-----------

CHAPTER 1

1.1 BACKGROUND

“We all provide personal information to organizations providing services – whether supermarkets, banks, local authorities or the NHS. We do so because we know that it helps them to provide us with a better service. But we also expect organizations to use that data responsibly, to keep it secure and to respect our privacy.” [Tony Blair, Foreword, Privacy and Data Sharing, 2002. pg. 2]

The driving force behind e-government is the need to create a more efficient government, using information and communication technologies to transform the structures and operations of government. The hope and potential behind e-government initiatives globally is the elimination of a fragmented public service by removing the silos that exist presently through the development of cross-departmental relationships. These relationships should result in the seamless provision of services to citizens. The secondary benefit from electronic government, and one, which will not be investigated into great detail for the purposes of this paper, would be to allow for increased citizen participation in the shaping of policy and to enhance the economic and social development through on-line access to government.

In South Africa the challenge of the digital divide is much greater than the United States of America (US) where e-government initiatives have been underway for some years and where ‘62% of citizens and 83% of business users ... had used the Internet to access government services or information.’ [McClure, 2000 Pg.2]. While the majority of South African citizens do not have access to the Internet, it will be some time before transactional and other forms of e-communication will be taking place amongst the general population. The vision for e-government is that it will enable easier access to

service and information from government by citizens, improve efficiency and effectiveness in the delivery of these goods and services to the general public and, last but not least improve government’s accountability and transparency.

There are a number of issues facing the success of e-government implementation globally. These issues include the expectation of citizens of privacy, security and trust in all transactions with government. Not only does government have to consider building privacy into technology architecture but also it should ensure that privacy issues are dealt with at the policy level, hopefully before the implementation of an e-government system. In the designing of technology it has to be remembered that technology is not neutral, neither is it a panacea for all society’s ills, including the protection of privacy. ‘Although it’s possible to use technology to protect or enhance privacy, the tendency of technological advances is to do the reverse. It is harder, and frequently more expensive, to build devices and construct services that protect people’s privacy than to destroy it.’[Garfinkle, 2001. Pgs. 258-259]

1.2 PROBLEM STATEMENT

This research paper will examine the potential barriers to e-government. One of the contentious risks to e-government globally is the issue of privacy. Unresolved privacy concerns are the biggest hurdle to e-government implementation today and the implementation for it in South Africa will be no different to anywhere else. These fears have not been resolved with the usage of e-commerce in the private sector. Although many people use the Internet on a daily basis to carry out online transactions, they resent

the fact that much of their personal information has been sold or passed on to third parties who inundate them with unwanted Spam. E-government will give online access to a range of information and applications and in turn there must be a balance between the demand for electronic convenience with the need to maintain security and privacy of data that is deemed sensitive. So herein lies the quandary that faces governments today.

This research will look at the imperatives of data management in order to ensure privacy and security of information. In the United Kingdom, data protection laws are seen by some to be hindering the progress of delivering seamless government services. This seamless delivery is done by what some call ‘joined-up’ or integrated government.

Joined-up government requires government departments to share data and information on citizens that at present is protected by data protection laws. E-government will naturally increase the amount of data shared between different government departments. As Canadian Privacy Commissioner, George Radwanski states, “It always sounds so appealing and seductive when people talk about merging databases, bringing down walls, and eliminating redundancy. Everyone wants cooperation and coordination between agencies that have a common goal. Everyone opposes duplication and waste.” [Crossing Bridges to Success, Pg. 1]. What this entails though is that without the natural silo walls of government, as we know it, ‘someone with a need to know only one piece of information can have access to lots more than he or she needs or has any right to.’

[Radwanski, G., Pg.2] ‘That’s one reason for silo walls. Another is that, without them, information can be combined; data can be matched, to reveal new information. That can

lead to profiling of citizens and that’s a distinguishing feature of surveillance societies.’

[Radwanski, pg.2]

Privacy does not only mean the protection of security and confidentiality. Privacy in the context of electronic government means the fundamental right as individuals to control the collection, use and disclosure of information about ourselves. The right to privacy means that individuals get to decide what and how much information to give up, to whom it is given, and for what it is used for. This is a key to this ‘inalienable right’ as outlined in the South African Bill of Rights. Confidentiality is an obligation to protect and keep secret personal information that has been entrusted to you. Information security on the other hand, is the process of assessing threats and risks posed to information gathered. It also entails taking the necessary precaution to protect this information against unauthorized accesses, use, loss or destruction of this information.

In addition, this study will give an overview of legislative attempts to protect privacy and in particular data protection and the reasons why legislation is just one of the many endeavors needed to ensure the success of e-government implementation. This Chapter will also look at the type of legislation and/or regulations that need to be promulgated to cover the areas of digital signatures and electronic records management. A legal framework will ensure that government departments will understand data-sharing and privacy issues while at the same time indicate how this information should be shared with the public.

1.3 OBJECTIVES OF THIS RESEARCH

The objective of looking at e-government and the specific issue of privacy would be to raise the debate on a subject, which has largely been ignored in South Africa. In order to stimulate this debate, some light has to be thrown on the following issues:

- The principal objective of this research is to examine and outline the causal link between e-government and the risk to an individual’s privacy;
- The secondary objective is to look at the roles and responsibilities of government to protect data while at the same time carrying out the necessary activities of e-government;
- The final objective of this research is to point towards areas of research that could not be dealt within the limitations of this study

1.4 LIMITATION OF THIS RESEARCH

This research was restricted because no empirical research was undertaken to ascertain whether or not privacy is a key issue within the South African environment.

1.5 RESEARCH DESIGN AND METHODOLOGY

The methodology used will be qualitative because various pieces of empirical research will be brought together to formulate a hypothesis, “In concrete terms, ... Qualitative analysis focuses on:

- Understanding rather than explaining social actions and events within their particular settings and contexts;

- Remaining true to the natural setting of the actors and the concepts within their particular settings and contexts;” [Mouton 2002, pg. 169]

The study will be using ‘inductive’ reasoning, which means that there has been previous research on the subject area and that the conclusion will follow the arguments raised from this research. But while there is a body of knowledge in the area of e-government and on privacy as separate research areas, not a large amount has been written on the two subjects in relationship to each other except in the specific area of data protection.

Inductive reasoning uses research as supporting evidence to reflect a certain situation; there is a great possibility that many other inferences can be drawn from that truth and the same data can be used to come to a different conclusion. “Empirical evidence that can provide support for the truth or likelihood of a conclusion must therefore be both ‘true’, or at least highly probably, and also relevant to the conclusion.”[Mouton, 2002, pg 71]

Secondary data sources in the form of published books, journals, as well as electronic papers, legislation and electronic journals have been used in this research. The Internet has been used for the greater part to view and download information from privacy sites and organisations like the Organisation for Economic Cooperation and Development (OECD) and other government sites that have produced a number of documents on both the subject of e-government and of privacy. On the whole the body of literature on e-government is not substantive and in the main published as papers on the Internet and in journals on public administration and government while the area of privacy, technology, surveillance is much more substantive and is well published.

Current research in the area of privacy in South Africa has in the main focused on privacy and e-commerce and the relationship between business and the customer. A search on South African Bibliographical Network (SABINET) on the terms "e-government" and "privacy", delivered articles on the technology aspects of dealing with privacy such as authentication, encryption or alternatively, e-government from a business point of view. A paper written by Julien Hofman, Associate Professor in the Department of Commercial Law at the University of Cape Town, on *E-Commerce and Issues in the Law of Privacy* again focused on the private sector. [Hofman, 2000] Another search on peer-reviewed articles on e-government delivered papers on the "digital divide", Information and Communication Technologies (ICT's) and government. *Cyberlaw: The law of the Internet in South Africa, 2000* has a chapter dealing with privacy and the right to information by Reinhardt Buys where it is stated in the introduction that, "the keys to further Internet growth, especially as far as electronic commerce is concerned, is the attainment of privacy through technology and law." Professor Britz of the University of Pretoria has written a paper entitled "*Technology as a threat to Privacy*", wherein he postulates on the threat that technology poses to privacy with no particular linkage to the South African situation.

1.6 OUTLINE OF CHAPTERS

- Chapter 1 outlines the scope of this study and the research design and methodology.
- Chapter 2 will give an overview of electronic government, its activities, its constraints and barriers as well as snapshot of e-government plans, policies and legislation in

South Africa. This chapter is necessary for the reader to understand the reasoning behind linking the risk to privacy directly in relation to e-government.

- Chapter 3 will attempt to define the meaning of privacy and the specific linkage to e-government and the information age.
- Chapter 4 will look at data and information and the protection and management thereof as well as the roles and responsibilities of government in safeguarding the data collected.
- Chapter 5 will suggest recommendations for policy and governance for the handling of data in South Africa

CHAPTER 2

E-GOVERNMENT

“There is nothing more difficult to undertake, more perilous to conduct, or more uncertain in its success, than to take the lead in the introduction of a new order of things.” [K. Ashok Vardhan Shetty, 2003, Pg. 1.]

2.1 INTRODUCTION

Governments are seeing e-government globally as a new way of interacting with citizens. There is a perception that e-government will transform the negative image of government “... as bloated, wasteful and unresponsive to their most pressing needs.” [Working Group on E-government in the Developing World, 2002, Pg. 1]. E-government can be seen as following the business model popularized by the private sector by turning itself into a ‘clicks-and-mortar’ business by using online activity to support its basic business. These online relationships do not replace the sometimes-necessary physical interaction that a citizen may require with government. “The impact of e-government at the broadest level is simply better government – e-government is more about government than about “e”. It enables better policy outcomes, higher quality services and greater engagement with citizens. Governments and public administrations will, and should continue to be judged against these established criteria for success.” [OECD, 2003, Pg.1]. This chapter will give an overview of e-government and its deliverables. To begin this process, one needs, to understand that e-government is about a new way of working and of delivering services and not just another technology system that needs to be implemented. “Only countries which are strong in governance and committed to reform can hope to succeed in their e-government efforts. Thus, it is not ‘e’ but the ‘government’ in e-government that is the significant part.”[Shetty, 2003, Pg. 3]

Globally, there have been a number of issues that have arisen out of online interaction with government. One of the most significant has been the one that affects the privacy of citizens and their information. Many governments are facing the quandary of having to

streamline citizen information in order to deliver efficient services, thus running the risk of having that information being altered in error or with a specific purpose in mind.

2.2 DEFINING E-GOVERNMENT

The 'e' in e-government stands for 'electronic' which means the ability of information and services to be transmitted over the Internet. In the literature on the subject, the word digital is quite often used interchangeably with electronic. There are many definitions of e-government and quite often e-government and e-governance are used interchangeably. For instance, a workshop entitled *Implementing e-Governance in Public Sector Organisations*", organized by the Commonwealth Network of Information Technology for Development (COMNET) was really about the implementation of e-government in the SADC region. While the term e-governance can be seen as the policies and the bodies implementing this new form of government.

There are numerous definitions of e-government but "but the actual government's objectives are indisputable: maintaining collective security, administering justice, providing the institutional infrastructure of the economy, ensuring that vital social capital is enhanced through improvements in health and education and through strong families and communities." [Tambouris, Gorilas, Boukis, 2001, pg. 2] These begin from philosophical perspectives to the description of e-government in similar economic terms as e-business within the private sector. Defining e-government is an essential component in implementing any e-government initiative or strategy. The process of defining e-government will give the term and process clarity, a common vision, and understanding as well as an intellectual frame of reference by which to eventually measure its effectiveness. I will review some of the numerous definitions found in the literature, which describe e-government, and along with these some of the expectations linked to these definitions.

The Canadian government clearly states that e-government is much more than a portal, much more than putting government online such as the Gateway portal that South Africa

is in the process of implementing. “Government On-Line is a precursor to e-government.... E-government will mean much more than putting existing Government-On-Line – [e-government is] a state of being where governments are interactive, inter-jurisdictional, fully connected to citizens, collectively working through issues and coming up with solutions to policy and program issues consistently and democratically.” [Dinsdale, et.al, 2002, Pg. 17].

The United Nations Division for Public Economics and Public Administration suggests the following definition: “E-government is a permanent commitment by government to improve the relationship between the private citizen and the public sector through enhanced, cost-effective and efficient delivery of services, information, and knowledge.” [<http://www.unpan.org/egovment2.asp>]

“According to another definition, e-government is the application of information and communications technology (ICT) to transform the efficiency, effectiveness, transparency and accountability of informational and transactional exchanges within government, between governments and government agencies at federal, municipal and local level, citizens and businesses, and to empower citizens through access and use of information.” [Tambouris, et al, 2001. pg. 1]

The provision of instant services to the citizen can be seen as superficial and instant gratification. A ‘quick-win’ situation while the long-term implication of e-government could have enormous consequences for both government and the citizen at large. “The challenge today is how to transition from an industrialized model of big government centralized, hierarchical, and operating in a physical economy to a new model of governance, adaptive to a virtual, global, knowledge-based, digital economy, and fundamental societal shifts.” [Caldow, 1997, pg. 1]

“The convergence of information gathering, processing and communications technologies has increased the capability of both government and private organizations to retrieve, recombine and disseminate information collected from a range of sources. These

organizations no longer regard traditional forms of information as confidential but see it as a commodity to be bought and sold for a reasonable fee”. [J. Whitaker & W.G. Hewett]

In its most limiting form, e-government can best be described as the provision of services reengineered by technology. “While others perceive e-government as a fundamental transformation of government and governance at a scale not witnessed since the beginning of the industrial era.” [Tambouris, Gorulas, Boukis, 2001, pg.1].

These varying descriptions of e-government give an idea of the differing expectations of the improvement of service delivery.

2.3 ACTIVITIES AND PRINCIPLES

E-Government is the ‘technologising’ of traditional manual processes that government sees as its governing role, e.g. the act of governing, regulation and monetary transactions, including tax collection, and the distribution of pensions to name but some examples. E-government is a paradigm shift in the delivery of goods and services to government’s customers using information technology. It is about the interconnectivity between civil society, public servants and business. It is about realising the true power and potential of an information society as well as making government more efficient internally, through improved communication, reduction of duplication and as mentioned before the automation of transactions [Blakely, 2001, Pg.1].

The drivers underlying e-government is the provision of public data, information and services to citizens and to other government departments as well as the improvement and efficiency in service delivery in all business areas. Government departments globally are beginning to understand the benefits of sharing information with each other thereby providing integrated services. This is what is meant by the often-used term – ‘seamless delivery’.

The activities and principles of e-government is aptly outlined in the following diagram taken from the US Department of Labour.

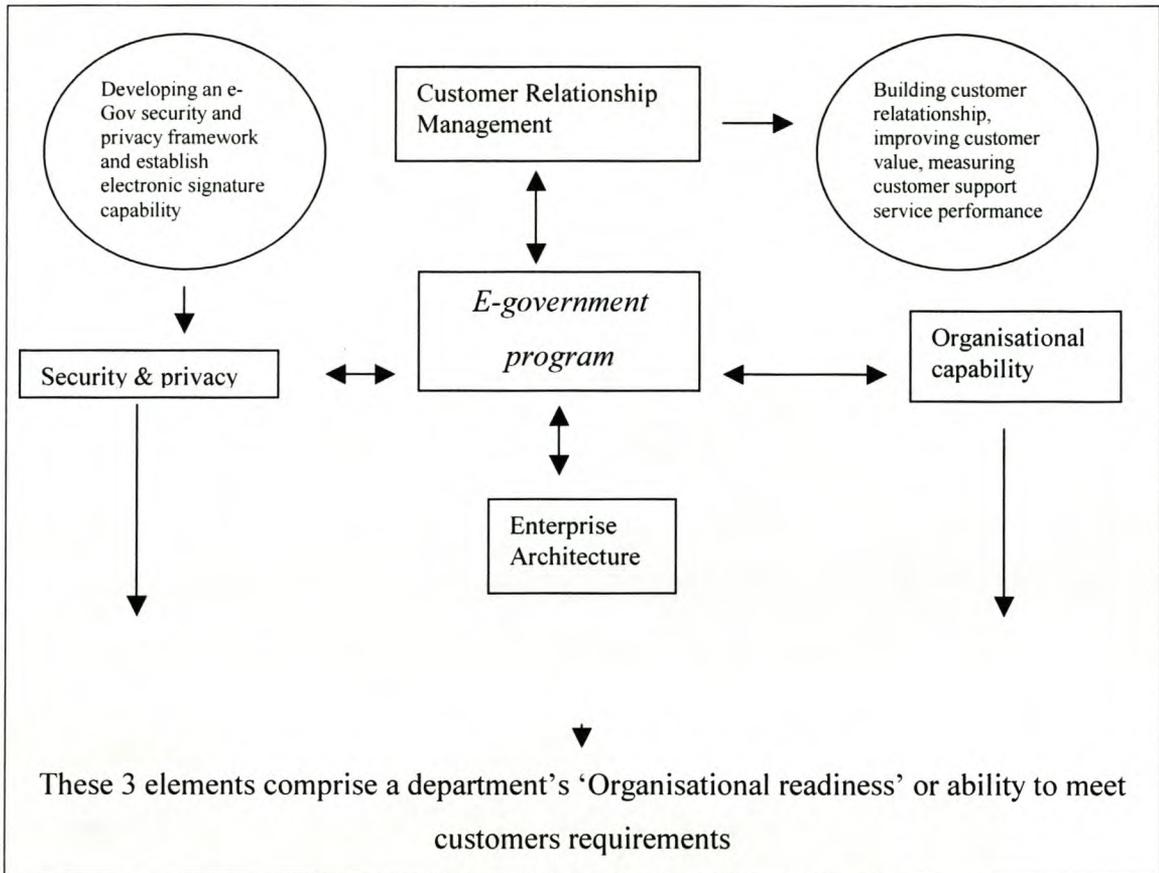


Table 1. Department of Labor, Office of the CIO, Affirm December 19, 2001

The three components of electronic government as outlined in Table 1 consist of customer relationship management, organizational readiness and security and privacy comprise an e-government program. To be successful, departments should make progress in all these areas simultaneously and in an integrated manner.

The activities and principles of e-government are far ranging. “Virtually every public policy area is going to be affected in this new Information Age, from security, privacy, intellectual property, copyright protection, universal access to how bit flows are taxed across networks that largely ignore any kind of political border. [Caldow, Pg. 5]

Citizens interact with government on a daily basis, whether it is to apply for an identity book, a birth certificate, a driver's license, a passport, to pay taxes, or receive some sort of social welfare benefit. These activities all generate an enormous amount of paperwork by both the citizens and the government department concerned. To finally receive these services, citizens have to wait long hours in queues and the procedure can be repeated on a number of occasions. For example the process of applying for an identity book in the South African context means waiting in a queue to fill in a form and hand over photographs and take fingerprints. These three activities often mean three different queues. Most working people have to take a day or at least a half-day off work to do this. Then when the citizen has been notified that their identity book is ready for collection, it will mean standing in another queue to collect the identity book. Many other services that are provided by government often mean that the citizen has to apply to a number of different departments for that particular service. E-government promises the citizen that there will be greater convenience because there will be a single point of contact with government. This point of contact will be available twenty four hours, seven days a week. Not only is this beneficial to the citizen but it frees up government to "redirect resources away from purely administration activities to concentrate on helping customers with complex queries or improving services to people from vulnerable sections of society". [Jupp, 2001, Pg. 1]

The common inference by the majority of authors on this subject is that e-government will enable government to become more efficient if more citizens can interact with it online. But it does not mean good government when tedious business processes are just given a new look by the use of technology. "An e-government strategy is not a conventional IT strategy which proposes technical solutions to a set of business needs. The business of government is too varied and complex, and the range of its dealings and contacts too great for that to be a sensible approach. Instead e-government should set a strategic direction for the way the public sector will transform itself by implementing business models which exploit the possibilities of new technology." [Zahran, n.d. Pg. 1] Business process reengineering is essential prior to the implementation of an information technology system because translating old ways of working will make a system

cumbersome and less user-friendly to all its users. The same principle should apply to e-government. If government's business processes are transformed, then it will be beneficial to all citizens and not only those who are able to access services online. By so doing, government recognizes the broader target population and does not limit itself to those who have access to a home pc or the Internet. "The impact of the digital divide will be much more severe if government services move exclusively online. [Klima, Pg. 4]

2.4 BARRIERS AND CONSTRAINTS

There are a number of barriers, constraints and risks to be taken into consideration for the successful implementation of e-government. These constraints can be looked at from two different viewpoints, i.e. that of the citizen and that of government. There are a number of constraints from a government perspective. The most cumbersome being the fact that government works within departments and not across departments. This problem is sometimes called the 'silo effect', which will be expanded on under 2.3.1 below. A secondary concern for government is the fact that government has the responsibility for generating, updating and managing huge amounts of data. The implications for government lie in surmounting this issue. From the citizen's viewpoint, the issues of the digital divide, and privacy and trust issues are the main concern.

2.4.1 Cooperation between Departments

Seamless delivery of services implies that government departments need to work closely together and that business process to some extent be integrated. "Their collaboration cannot merely be technical, but must involve a deeper engagement in terms of shared customers." [OECD, 2003. Pg. 5] There are a number of different levels of integration that need to take place. The first level of integration would be to remove all the technology silos to ensure interoperability, thereby creating a networked organisation within government. The second level of integration would be the elimination of redundant business processes to ensure that that finance, human resources and provision are going to meet the requirements of an integrated government. The third level of

integration would be for government departments to commit themselves to sharing information across the board. An example of the type of information that would be essential across government would be the correct contact details of a citizen. It is this aspect of information management that has the most impact on the privacy of a citizen.

2.5 E-GOVERNMENT PARADOX

What does the citizen expect of e-government? From the Hart-Teeter poll taken in the USA, it was deduced that there are a number of expectations of e-government. [Hart-Teeter, April 2003] The first one being the ability to carry out transactions online, i.e. paying traffic fines, registering a birth and/or death, filling out tax returns and other forms and applications. The second expectation being access to government information. The third, greater government accountability. "This was chosen by a considerable margin, almost three times as often as was convenient services. The second top priority according to the poll is convenient services. The third top priority according to the poll is greater public access to information". [McDermott, P. 2000, Pg. 2].

The Hart-Teeter poll reveals that American citizens believe that 'moving citizens out of line and online' will profoundly change the relationship between citizens and the state. It was also noted that it would provide easier access to information held within the public sector. While transforming from within by increasing efficiency and cutting down on costs, it will at the same time be able to provide a faster and more responsive service to the citizenry. The paradox lies in that in so doing the above, the state will increasingly be able to monitor citizens more closely than before, if only to carry out its tasks more efficiently, for example the provision of social welfare services.

The paradox that becomes clear is that while a Joined-up or coordinated government will definitely improve administrative efficiency, it will at the same time collect an inordinate amount of information on citizens, thus creating profiles of a populace that is generally unaware of this collection of personal information. "As the state becomes a more efficient, and voracious, information consumer, the danger of the state abusing this

information also grows. This threat has been addressed by Freedom of Information and Data Protection legislation in many jurisdictions. These provide safeguards against abuse of the state's store of information about citizens." [Quinlan, Buckley, Schon, Harris, 2001, Pg. 13]

2.6 THE SOUTH AFRICAN SITUATION

In South Africa, the move to more efficient government began by using an IT strategy and focus as outlined in the Electronic Government policy framework put out by the Department of Public Service and Administration in 2001. [DPSA. February 2001]. The second stage was to introduce Information Technology Planning Guidelines for all government departments [DPSA, 2002]. Information Technology planning ensure that the business objectives and strategies of each of these departments informs the choice of technology used. These Guidelines also encourages "... consistency in Information Technology planning and documentation." [DPSA, 2002. Pg. 4] Another objective of these Guidelines is to study the data collected and how it is maintained and archived.

2.7 CONCLUSION

The conflict within e-government lies in the trade-off between convenience and security. The maintenance of privacy is one of the critical success factors in the successful delivery of e-government. In the Western world, the two main concerns around e-government are how the public view e-government impact on their privacy and the security of their information. Recommendations and some practice include privacy policies posted on web sites. Citizens need assurance that their data will be used for the purpose for which this data is collected. "In an era of big business and big government, when product innovation can be copied in weeks and reputations can be ruined in minutes with slick multi-media campaigns, trust is increasingly the currency of a relationship." [Don Peppers and Martha Rogers, 2002. pg,1]

It is a common experience for both Internet and non-Internet users to find that their personal information has been shared or sold to other companies. Government has to be careful how it collects personal information and what it does with this information. While there is no legislation in South Africa regulating how the private sector or government manages personal information, an issue paper has been circulated by the South African Law Commission on Data protection. A basic premise of successful e-government is the maintenance of privacy and the creation of trust in government's ability to manage personal information.

CHAPTER 3

PRIVACY

3. 1 INTRODUCTION

“We stand at the brink of an information crisis. Never before has so much information about so many people been collected in so many different places. Never before has so much information been made so easily available to so many institutions in so many different ways and for so many different purposes.[Simson Garfinkle, 2001]”

The elements of privacy and trust are contentious issues in the implementation of e-government. The literature shows that the risks of an integrated, information-sharing government, where paper-based processes are exchanged for electronic processes becomes a barrier to the future success of e-government. Privacy is considered as important and stands alongside access and efficiency as a priority and a requirement of good governance. Most governments are dealing with this by using technology to safeguard data, but privacy-enhancing technologies can only go somewhat towards the protection of personal information. Technology needs to be guided by values and principles otherwise the following fictional scenario could happen: “As an ambulance rushes an unconscious patient to the hospital, doctors prepare to save him by accessing an online database with data on his pre-existing heart condition. During the same month, people with similar heart conditions are denied jobs when prospective employers gain access to a similar database.” [Mechling, Applegate, 2001, Pg. 1]

The right to privacy has on the whole not of any special significance for the ordinary South African, who for the most part is disinterested in the notion of privacy. There are too many competing priorities that absorb the attention of the majority of South Africans in as far as rights have been concerned. These have included the right to housing, land, education and all the other rights as set out in the South African Constitution.

3.2 DEFINING PRIVACY

The concept of privacy has to be defined in order to understand how electronic government affects it. There are numerous definitions of privacy. Privacy is recognized as a human right and is enshrined in numerous international human right treaties and agreements. "The right to privacy is guaranteed expressly in the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, the American Convention on Human Rights" as well as in many countries constitutions, including South Africa. [Buys, 2000, Pg. 365-366.]

The traditional or social definition of privacy was seen in the context of an individual left alone to his own devices and protected from unwanted and unauthorized intrusion. The legal interpretation of privacy has been described as "...the right to be free of unnecessary public scrutiny or to be left alone." [Baker, Akridge, Christensen, Keck, 2002, Pg. 6] In many countries, the concept and definition of privacy 'has been fused with Data Protection, which interprets privacy in terms of management of personal information.' [Baker, Akridge, Christensen, Keck, 2002, Pg. 5]

The Global Internet Liberty Campaign (GILC) [Baker, Akridge, Christensen, Keck, 2002, Pg. 6], suggests that the privacy aspects which are of concern to e-government can be divided as follows. Information Privacy – which would be the rules to govern the collection and handling of personal data such as credit information and health records; Privacy of Communications - which encompasses the security and privacy of mail, telephone and email; Territorial Policy – which sets limitations on intrusion into the private domain, the workplace and/or public space;

The concept of privacy has moved from its original portrayal as "The right to be left alone" to the modern-day understanding and request from citizens, that government and other entities (such as the media), allow individuals to go about their daily lives without the fear of intrusion, monitoring and surveillance. With the advent of e-government, the interest in privacy would be related to an individual's concern over government and other

individual's accessibility to our most private lives. The ability to capture, translate and retransmit data in today's world has altered the privacy paradigm.

3.2.1 Information Privacy

Privacy needs to be understood within the context of security of information. This encompasses the concept of data protection. Privacy of information is affected by the ability of both government and the private sector of mining enormous amounts of personal information. "Definitions of privacy vary widely according to context of environment... In many countries, the concept has been fused with Data Protection, which interprets privacy in terms of management of personal information." [Baker, Akridge, Christensen, Keck, 2002, Pg. 5] In the context of electronic government, the flow and subsequent collection and storage of data have consequences upon privacy. Data protection is essentially the rules that govern the collection and handling of personal data. Data protection legislation requires that governments treat personal information in the following manner: "... personal information be obtained fairly and lawfully; used only for the original specified purpose; adequate, relevant and not excessive to purpose; accurate and up to date; and destroyed after its purpose is completed. [Banisar, Pg. 7]. Protecting citizen's privacy rights in the e-government context would mean giving them more choice in the management and use of their personal data. There should be openness, transparency and consultation in cases where data is used and shared without permission. A balance has to be struck between individual's rights and the wider public intent. Ongoing monitoring and assessment should happen in regard to the benefits of data sharing and alternate approaches should be sought and safeguards should be put in place such as privacy enhancing technologies.

3.2.2 Communications Privacy

Privacy of Communications encompasses the security and privacy of mail, telephone and email. This privacy right is delineated in the European Convention for the Protection of Human Rights and Fundamental Freedoms 1950 which states that "everyone has the right

to respect for his private and family life, his home and his correspondence ... and that there shall be no interference by a public authority” [Laurant, 2003, Pg. 5] unless, it is deemed to affect national security, or it is necessary to prevent crime or it affects the rights of others. In direct reaction to the increase in communication technologies, many governments have introduced wiretapping laws to increase surveillance capabilities and permissions. An example of this is the South African Interception and Monitoring Act of 2002 which is intended to regulate the interception of certain communications, the monitoring of certain signals and radio frequency spectrums and the provision of certain communication-related information as and when needed by law enforcement agencies. These laws are posing new threats to privacy because new technologies are enabling a greater increase in the information that government are able to tap into. Wireless technologies and Internet usage means that authorities are able to gather more information on an individual at a rapid rate through tracking the sites that are visited and their transactions carried out. Wireless “provides details of an individual’s movements and activities and whom they have met.” [Laurant, 2003, Pg. 25] Profiles on individuals are put together with ease by collecting and analyzing information that is a byproduct of transactions carried out over the Internet.

3.2.3 Territorial Privacy

In today’s global economy, “... there is an emerging geographic incongruity between the reach and domain of the state and the deep and dense network of transnational economic relations.” [Kobrin, 2002, Pg.1] Territorial privacy encompasses electronic intrusion across country boundaries because of the effortlessness of Internet transactions. This means that information on individuals can be gathered from anywhere in the world. The European Union 1995 Directive on Data Protection attempted to “protect the data privacy of Europeans regardless of where data is transferred and processed.” [Kobrin, Pg. 3].

Location information generated by mobile telecommunications provides details of movement and activities of individuals. This information combined with any transactional information on the Internet and tracking of websites visited can be used to

create a detailed profile. The European Union has legalized the data collected through communications technologies through the Electronic Communications and Privacy Directive of 2002 even though this policy is “in direct contravention of data protection practices of deletion of data once it is no longer required for the purpose for which it was collected.” [Laurant, 2003, pg. 28]

Territorial privacy also covers surveillance of the workplace and public spaces in general through audio and video technologies, as well as the monitoring of email usage and Internet searches. Employers have always collected information on workers but usually with their consent. With new technologies, workers basic rights to privacy are in danger of being encroached upon. These new technologies can “record keystrokes on computers and monitor exact screen images, telephone management systems can analyse the pattern of telephone use and the destination of calls, and miniature cameras and ‘smart’ ID badges can monitor an employee’s behaviour, movements and even physical orientation.”[Laurant, 2003, Pg. 60]

3.3 PRIVACY IN THE SOUTH AFRICAN CONTEXT

The privacy right as mentioned in the South African constitution ‘protects information to the extent that it limits the ability of people, organisations and the government to gain, publish, disclose or use information about others’ [Buys, Pg. 367] but this right is not deemed absolute. The South African government has to reasonably justify the collection of information which is necessary for statistical or census purposes while at the same time refrain from bypassing the right to privacy.

The South African Law Commission has put out for discussion, an issue paper entitled “Privacy and Data Protection”. This issue paper will be the basis for legislation on this subject. The need for legislation on privacy and data protection arose from the Promotion of Access to Information Act of 2000, which dealt with access to personal information but did not elaborate further on the privacy implications of the collection of this data. Neither did it deal with the ability of citizens to correct wrong data.

The intent of this proposed legislation “is to ensure that government and private organisations accord personal information an appropriate measure of protection, and also that such information is collected only for appropriate purposes and by appropriate means.” [Howie, 2004, Pg. 8]

South Africa has had an identification strategy for many years whereby citizens are required to apply for an Identification book at the age of 16 which is imprinted with an identification number given at the registration of birth. This identification book is needed for the rest of a citizen’s natural life for all types of requests both from government and the private sector such as identification when opening up a bank account and many other transactions. Since September 11, the USA is now implementing measures “... to increase security against terrorists through the collection of personal information, tracking of movements and identification technologies.” [Mladen, 2003. Pg. 274.

3.4 INFORMATION FOR GOVERNMENT

What information does government need in order to rule? Before this question can be adequately answered, there has to be some understanding of what drives government. This is aptly illustrated by Thorson [in Caldow, 1997, Pgs.10-11], “Much of what drives the demand for technology in the United States is an emphasis on efficiency, or doing more with less. In other parts of the world, technology is primarily driven by information – how information is controlled and distributed ... the focus on information may be more valuable than the focus on efficiency... as we can become highly efficient in doing the wrong things.”

The task of government to govern, to provide services and to enable various forms of transactions to take place means that information is gathered, stored and dissected. With this responsibility, the citizen places trust in government’s ability to use this information with privacy considerations in mind.

The future impact of inter-departmental partnerships, systems, relationships and networks will be phenomenal especially in the area of information sharing. Data will also be put to better and more efficient use due to greater expectation put on information and record management. “When the public sector can achieve improvement in services or efficiency without requiring more data and affecting personal privacy it should do so, recognizing that the protection of privacy is itself a public service.” [Cabinet Office, 2002, Pg. 5]

Data sharing, if done from the citizen’s point of view, would always look at the actual benefits to individuals rather than the benefit to government. Strategies should take into consideration the building of trust. Thus, government should not just collect information without analyzing the importance and intelligent use of personal data without recognizing the formal rights and legitimate expectation of the protection of personal data.

Mr Jeffrey Eisenach, President of the Progress & Freedom Foundation in Washington has predicted that sooner or later, a state web site in the USA would be broken into and that government owned data on perhaps 200,000 citizens, such as personal information about child support payments, taxes, criminal histories or driving records would be accessed and posted on the web. In the USA, questions regarding privacy are becoming a priority for federal states as more and more government functions go online. In 2000, the Federal Office of Drug Control Policy used profiling cookies to collect data on visitors to its web site. This was one of several incidents that raised concerns about how government collected personal data online and whether government should be trusted with personal information. This type of incident and of many others has meant that privacy proponents have called for the strengthening of the US Privacy Act of 1974. E-government aims eventually to integrate all government data banks. Databanks which when put together have enormous amount of information on the individual. This integration will challenge the interests of individual privacy.

3.5 CONCLUSION

Privacy is an age-old issue the Information Age where it is easier to access, store, manipulate and retrieve information has brought privacy protection to the fore as a public policy issue. “The position that we all deserve privacy on a humanistic level is abstract. The position that individual interests can be harmed when personal information is processed inappropriately, especially if that position is supported by well-chosen horror stories, can have a more direct political appeal.” [Bennet, 2001, Pg. 5] Expectation is that sensitive information about citizens must be identified and appropriately protected. Yet a joined-up, ‘efficient government’ actually raises the specter of ‘big brother’, of a society whose surveillance of the individual would be substantially strengthened and where it would be so easy to misuse this knowledge and ability

Everybody will agree that the advent of e-government means that the ability to communicate and obtain information electronically will be at an unparalleled level within government as we know it. Much of the discourse on e-government has consensus on the fact that the invasion and disregard for an individual’s privacy rights is one of the main challenges facing governments today. Herein lies the paradox that they are forced to acknowledge the fact that, “our capacity to create surveillance societies should force us to confront fundamental questions about their desirability, but often the pressure for economic efficiency and effectiveness overpowers any pause to consider the human values that are being trampled, especially by governments and legislatures.” [Flaherty, 1989. Pg. 6]

The following chapter will look at the issues of the collection of data and its impact on privacy and security of information and make some recommendations to the way this can best be managed.

CHAPTER 4

PRIVACY AND DATA MANGEMENT

“Our capacity to create surveillance societies should force us to confront fundamental questions about their desirability, but often the pressure for economic efficiency and effectiveness overpowers any pause to consider the human values that are being trampled, especially by governments and legislatures.” [Flaherty, 1989/ Pg. 6]

4.1 INTRODUCTION

Privacy is not something that is particularly unique to the use of technology in government or the private sector but it is definitely being made easier and more efficient for large institutions to compile enormous amounts of data and information about any one individual. Some will argue that there should be no fear of this by product of a digital world while others will begin to realize how easy it is to compile profiles of individuals; how easy it will be to connect the wrong data to an individual by inputting wrong information; and how easy it will be to make assumptions about an individual based on this information.

There are a number of security issues arising out of electronic government that will impact on privacy. These issues range from the requirements of citizens carrying out business with government; civil servants access and treatment of data; encryption of data; information classification; data collection and retention procedures; data protection policies or lack of them; the rights of citizens to be able to correct their data and, last but not least, inter-governmental sharing of information. This Chapter will specifically focus on the responsibility of government in regard to the direct management of data. This includes the envisaged collaboration between government departments in the sharing of data. It will also focus on the policies that will be necessary to be put into place to ensure that data is protected and that citizen’s privacy rights are safeguarded.

4.2 DATA MANAGEMENT

4.2.1 What is data management?

“Government has special privacy obligations arising from the handling of sensitive information, its special position of trust, the huge power difference between Government and citizen, and the fact that government is a monopoly service provider – customers are obliged to deal with Government for many services.” {Riley, December 2000, Pg. 10]

There are three primary data management issues facing e-government today and these are data collection and retention procedures of government departments, the ability to share information between government departments and the third is the right of citizens to know what information is held by the state and to be able to correct that information if necessary.

Data management procedures should be seen from the perspective of privacy. “Record management practices and retention require the identification of confidential information and the establishment of procedures for protecting it.” [Department of Information Resources, Texas, 2000. Pg.10]. Identification and authentication applies to the transactional aspect of e-government where there is a real need to be able to identify who is requesting and receiving a particular service such as a birth registration or a hunting license.

E-government, as mentioned previously will transform the way data and information is collected, stored and used by government entities. Data management and protection are not new concepts to the management of government information. The e-government goal of delivering seamless integrated government services to citizens will mean increased sharing of information between the various branches and departments of government. This goal aims at eliminating “duplication of effort and achieve economies of scale in the course of transferring data between governmental bodies.”[Department of Information Resources, Texas. 2000, Pg. 11]

Data management and protection are not new concepts to the management of government information. But a definite aim of e-government is to provide seamless integrated government services to citizens. This should and will mean increased sharing of information between the various branches and departments of government, thereby increasing efficiency and eliminating "duplication of effort and achieve economies of scale in the course of transferring data between governmental bodies." [Department of Information Resources, Texas. 2000, Pg. 11]

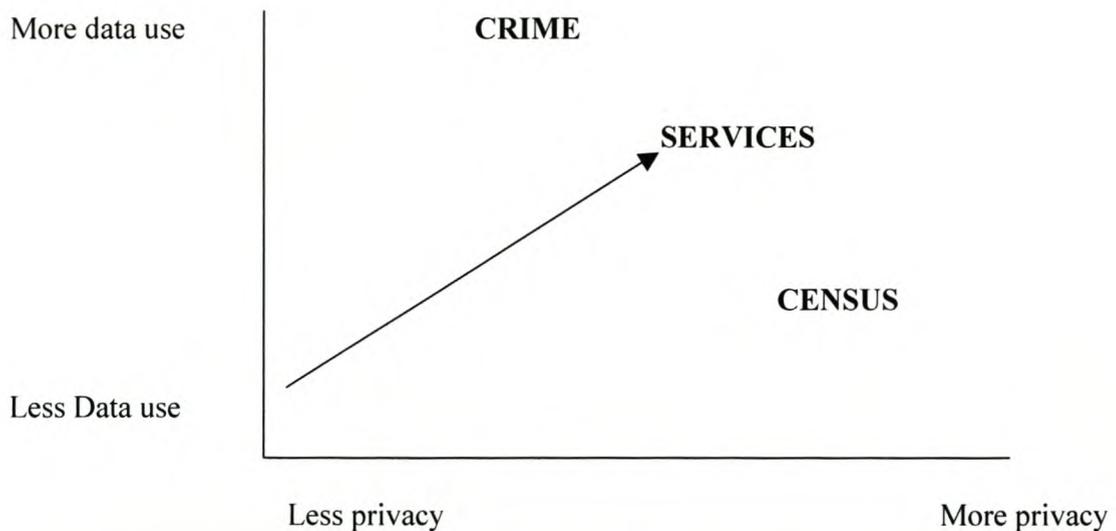
Data management procedures should be seen from the perspective of privacy. "Record management practices and retention require the identification of confidential information and the establishment of procedures for protecting it." [Department of Information Resources, Texas, Pg.10]. The concern for citizens would be would be the linking of different data to their names. For example, the amount of traffic fines they have incurred or whether they have defaulted on payments or whether or not they have been tested for HIV. The list could be endless. The implications and possible repercussions of all this information linked to one person could be enormous especially if any person or organisation were looking for such information. The inefficiencies of government have up to now allowed many of the different facets of our lives to go pretty much unnoticed and unconnected.

Data on citizens is collected without any due thought or deliberation on whether or not this collection is necessary for the provision of services. In the USA and other countries, citizens have been greatly concerned about whether government will be efficient and sensitive with their information, such as medical information and whether or not the law can protect them in the event of confidentiality being breached. An example of where data should be reliable at all costs would be an electoral register. The assessment of the quality of data for an electoral register would be the assurance that all information is at the very least complete, i.e. that it covers the entire population of eligible voters and this information is accurate. This completeness and accuracy is usually assessed every five years at national elections. If information was gathered and matched on a continuous basis, then accuracy would be greatly increased.

In April 2002, the UK Cabinet Office produced a report entitled “Privacy and Data-sharing: the Way Forward for Public Services”. This paper made recommendations on the improved use of personal information collected by the public sector to deliver better services to citizens. It also recommended that a concerted effort would have to be made to develop public trust in the way personal information would be used. These recommendations include:

- (a) Clear privacy statements both on government web sites and in public places;
- (b) Codes of practice on data sharing available to the public;
- (c) Publicly available information on how to access personal data with clear access request procedures;
- (d) Publicised information on how to deal with complaints about personal information;
- (e) A responsible individual’s name is published all government information pamphlets, web sites, etc. to handle personal information;
- (f) Campaigns to be run to promote public awareness of their rights and obligations;
- (g) Regular audits to be done data accuracy and reliability;
- (h) Technology standards across government on information security;
- (i) Legislation to be introduced to enable public bodies to share personal data more flexibly;

Privacy and the collection and better use of data are not mutually exclusive goals for e-government. As described in the table below, it is essential to have the correct data whether collected for census, elections or crime statistics. In the same UK report on Privacy and Data-Sharing in April 2002, it was perceived that increased data sharing by different areas of the public service would be detrimental to data quality for example: “with wider access and use, external – i.e. users outside the department which originally collected the information – or inexperienced users may create errors; with increased external use, there is greater potential to spread errors; and, the existence of multiple users may blur ‘ownership’ of the database and with it the loss of responsibility to supervise database practices and maintain quality.”[UK Cabinet, 2002, Pg. 71].



Performance and Innovation Unit, Cabinet Office, UK, April 2002. Pg. 51

The graph depicts the supposed relationship between “improved use of identifiable personal data and increased privacy. In some instances – such as crime – it may be possible to achieve the same level of privacy as in the delivery of other mainstream services. By contrast, in areas such as the census, confidentiality is fundamental to the services. However, in many public services, business processes, technology and system design can deliver privacy and better data use in equal measure – the arrow therefore suggests that, in general, public services should be moving towards the top-right quadrant in their approach.” [Cabinet, Pg. 51]

4.3 DATA PROTECTION

The need for protection of this information and data is recognized in many countries. Data protection legislation has been enacted in Canada, the European Union, the USA and the United Kingdom. This legislation protects an individual from the use of information that is inaccurate, incomplete or irrelevant and it protects personal information from being accessed by unauthorized bodies and individuals. This means

protecting the use of information in a context or for a purpose other than that for which the information was collected in the first place. This Charter is attached to the end of this paper as Appendix A. The UK Data Protection Act of 1998 (DPA98) allows individual to greater access to their personal information. This Act proposes that a National Information Commissioner oversees the recommended Charter on Data Protection and the Act itself.

4.3.1 What is Data Protection?

Flaherty describes data protection as “ an aspect of privacy protection that is especially involved with control of the collection, use, and dissemination of personal information. Data protection is implemented to limit this type of surveillance by other persons and organizations and thus to preserve individual privacy.” [Flaherty, 1996. Pg. Xiv] The European Union Working Party on the Protection of the individual with regard to the processing of personal data, ‘stressed the importance of ensuring that adequate means are put in place to guarantee that individual ... users get all the information they need to place their trust, in full knowledge of the facts, in the sites with which they enter into contact, and if need be, to exercise certain choices in accordance with their rights under European legislation.” [Article 29 – Data Protection Working Party. 2001. Pg. 2]

4.4 DATA SECURITY

Information security is the responsibility of ensuring that personal information and transactions are secure from third party theft and/or manipulation. Security is often breached from the inside of the civil service rather than the great fear of hackers from outside of government. “Governments are faced with more serious challenges than business, in the area of security, because accountability can be even worse than bankruptcy.”[Riley, 2003, Ph. 14] Examples of possible security breaches could be surreptitiously viewing data when not necessary in the carrying out of a duty; taking work out of the office in order to complete a task; “The only way to maximize information security is when every member of the organization, from top to bottom, buys in to the

goal of information stewardship.” [Riley, 2003, Pg. 14] Public employees need to buy into the confidentiality paradigm to prevent unauthorized disclosure of confidential information. “Information management is a human endeavor rather than a technical task.” [Riley, 2003, Pg. 23. A large part of the information management task is to ensure that the civil service undergoes a radical shift in the type of people that are being employed, a shift which recognizes that the ‘stayers’ are not necessarily the ones that should the ‘doers’ of this information age.

4.4.1 Digital Signatures

One of the steps necessary to ensure that electronic transactions are safe is the recognition of digital signatures. Legislation should ensure that digital signatures are as legally binding as traditional signatures. There is often a competing interest between security and privacy. The issue is to ensure individual privacy while at the same time maintain national security. This means that government should have a way to tap into individual communication if deemed necessary in the national interest. Ensuring security is a technical issue and privacy rights are a philosophical/legal policy issue. Private data of individuals should be precisely identifiable so that it is secured.

Government departments across the board should have the same security classifications so that what is recognized as private in one government department is not public in another. To categorise data coherently, the following guidelines should be adhered to:

- Data/Information should be considered internally restricted i.e. it can only be accessed by one department;
- Data/Information is considered conditional restricted i.e. not available publicly but can be shared between government departments;
- Data/Information is considered conditional public i.e. exposed to the public after a certain period of time or available on a need-to-know-basis;
- Data/Information should be considered publicly available;

4.5 SOUTH AFRICAN EFFORTS AT DATA MANAGEMENT

South African government departments are in the process of beginning the conversion of paper records into electronic data systems primarily to improve internal business processes. By default this would ultimately benefit and enhance the relationship with citizens through the timely response to information requests and to correspondence in general.

The South African Access to Information Act of 2002 requires that each government department provide an Information Manual for public access. This leads us to ask the question, “what are the obligations of government to protect the integrity of data, yet comply with other types of policy constraints such as open records law and the requirement of public records?” [Baker, Akridge, Christensen, Keck, 2002. Pg. 2] The Information Manual indicates what information is publicly available, available on request or secret and confidential. So legislation has to some degree begun the process of government identifying and classifying (organizing) information, both personal and otherwise into easily accessible document management systems. The problem with this piece of legislation is that even though it allows greater access to government information, government response is more often than not from a defensive and protective standpoint.

The next step in organizing the business back end of government would be to develop a single common file plan for the whole of government. By recognizing that information is a valuable asset and developing a common understanding, government is beginning to recognize the importance of information.

4.6 POLICY AND LEGISLATIVE MEASURES

In a country which is trying to sort out identity issues based on class and colour, the philosophy of privacy has not yet begun to permeate society as an “inalienable right” even though it is mentioned in the South African Bill of Rights. “Privacy isn’t just about

hiding things. It's about self-possession, autonomy, and integrity.' [Garfinkel. 2001, Pg. 4]. "Privacy is fundamentally about the power of the individual.' It is about how 'Institutions and the people who run them use technology to gain control over the human spirit, for good and ill.' [Garfinkel, Pg. 5] It is in fact not technology, which breaches our privacy rights, but the way technology can be, and is, used in many contexts that violate privacy rights. The lack of, or alternatively, the proliferation of policy and legislation does not always cover adequately the fundamental aspects of privacy.

There is no single uniform solution. It should be a "mix of regulatory and self-regulatory approaches blending legal, technical and educational solutions that suit the legal, cultural and societal context in which they operate holds the promise to provide effective solutions that, beyond the objective of building bridges, to the actual integration of different elements into viable solutions." [OECD, 2003. Pg. 4] It is essential to involve all sectors of society in policy and legislative development for the successful implementation of privacy measures, including business and lobbying groups.

The scope of the proposed electronic government Act is to cover all internal e-government administration, inter e-government administration and electronic interaction between government and civil society. The proposed objectives of the Act are to create a Gateway (portal) and call centres and to provide e-government services through this Gateway. The Act will also regulate methods of authentication and identification of users using a smart card. The Act will also provide for the integration of all public body web sites. The Act will regulate the provision of e-government services and the interoperability and security standards of technology used. The Act also proposes the setting up of a separate company to manage the Gateway.

At present in South Africa, there is no specific legislation protecting both citizens and the state with regard to the use of electronic information technologies. There is draft legislation being drawn up by the State Law Advisor but for the present time, individuals would have to have recourse to general constitutional law in this regard.

Governments are beginning to grasp that intelligent data collection is a central component to enable delivery of services to the public. Policy development in the area of privacy should clearly outline concepts such as what data should be collected about individuals; Who should be notified of collected data; conditions under which data should be stored; the right of individuals to access and call for corrections to stored data; and the limits to use and disclosure of stored data. [Whitaker, Hewett (2000). Pg. 4]] The National Archives of South Africa Act, 1996 (Act No. 43 of 1996) defines a record as recorded information regardless of form or medium and charges government departments with the proper management and care of all public records in their custody. This Act’s main objective is to preserve public records but no mention is made of privacy measures. In the Guide to Management of Electronic Records in Government Bodies published in 2000, it is noted that technology “can manipulate large amounts of information and generate a wide range of information products” and that “the unique and fragile nature of electronic data demands a reevaluation of the way governmental bodies manage records.”[National Archives of SA, 2000, Pg. 1].

Governments globally are either in the process of developing their Data Protection Legislation or enacting them alongside other legislation which impact on privacy such as Human Rights Acts, Privacy Acts and Freedom of Information Acts, Access to Information, Electronic Transaction, E-government Archives and all other legislation impacting on information.

At the present time, there is no legislation specifically focusing on privacy in South Africa. The only legislated mention of privacy is Section 14 in the Bill of Rights which states that “Everyone has the right to privacy, which includes the right not to have – (a) their person or home searched; (b) their property searched; (c) their possessions seized; or (d) the privacy of their communications infringed.” [The Constitution of the Republic of South Africa, 1996]

But subsequently, there has been a creeping in of legislation that may and will to some degree impinge on this human right. Legislation such as the ‘Regulation of Interception

of Communications and Provision of Communication-Related Information Act, of 2002, the Electronic Communication Transaction Act of 2002. Other legislation that is at present being drafted by the South African Law Commission includes an E-government Bill

4.7 CONCLUSION

The paradox for e-government is that while its intent is to provide seamless services and improving delivery of these to all citizens. In the process of doing this, the state will at the same time be accumulating massive amounts of information on individuals. This collection of data needs to be managed in such a way so as not to allow for the very real danger of abuse. This abuse could take various forms, whether it could be in the manner of linking the wrong information to an individual either in error or purposefully to destroy a reputation. Mismanagement of data and information could also eventually lead us full circle back to inefficient government where data and statistics become meaningless without the necessary strategies, policies and legislation in place.

E-government involves the collection, use and disclosure of personal information, which in essence means that it is about issues of privacy. Providing greater access to information makes a huge assumption that government has high performance data storage and the requisite tools to locate information and reliable and secure networks and software to deliver and protect critical information. While the South African government together with the State Information Technology Agency (SITA) is working very hard at producing the above, which will enable the future provision of information to be smoothly enabled, there will be no accounting for past information that needs to be accessed.

The question as to whether their information is sufficiently protected under any legislation that is currently in place. The South African Law Commission is drafting a privacy bill and an e-government Bill for consideration in the next session of Parliament. These pieces of legislation will hopefully cover all the loopholes left in other legislation

such as The Access To Information, The National Archives, Electronic Communications and Transaction Acts.

The issue of privacy, data protection and electronic records management needs to be addressed preferably at the early stages of e-government implementation. It is an opportune time for policymakers and legislators in South Africa, to be aware of these issues and take them into consideration. The implementation of record management policies as well as the necessary training of public service employees in the collection, maintenance and privacy considerations of data is essential for the security of information.

CHAPTER 5

CONCLUSIONS AND RECOMMENDATIONS

“Basic legislative responses. Turn out to be counterproductive ... and legislating a new media, the Internet, without understanding its inherent characteristics places any government at risk t in the electronic frontier”. [Janet Caldwell]

5.1 INTRODUCTION

This research paper has given an overview of the issues affecting privacy within the e-government context with the objective of raising the debate on the matter and hopefully providing some insight and the need for more in-depth research into this area of study..

5.2 SUMMARY OF LITERATURE REVIEW

5.2.1 E-government

Chapter 2 looks at how e-government transforms the manner in which services will be delivered by government to citizens. By providing these services online through a transactional relationship, government hopes to be quicker and save money. This will also mean changing the way government works internally by changing bureaucratic methods of working and by changing paper processes into systems. By moving into the electronic environment, government will be able to lessen the duplication of information that occurs with normal government because it will ease the sharing of citizen information between the different sectors.

5.2.2 Privacy

Privacy is recognized globally as a human right and is protected in various declarations and conventions that deal with human right issues. Prior to the development of communications and other technologies, privacy was understood to be the line or cut off

point between society and the individual. It was the recognition that the state could not intervene in citizen's personal affairs unless these affairs were considered a security risk to the general populace and/or him/herself. Privacy ranges from impact on information to the security and privacy of communication devices such as telephones and email, to the abuse of privacy in the work place and across sovereignties and borders because of the rapid evolvement of the Internet as a communication and transactional tool.

The ability of government to amass enormous amounts of data and information on citizens have abounded and become more efficient in the electronic environment. There is a definite tension between the simplifying of business processes and the expectation of information privacy.

5.2.3 Privacy and Data Management

The management of information is becoming a central tenet of e-government. Service delivery can only be improved if information is stored and organized efficiently and accessed electronically across a 'joined-up' government. Data security measures are imperative, both through technology encryption software and through specific policies. It is also crucial that public sector employees are aware of the import of dealing with data and the impact on privacy of the incorrect data being inputted into a databank.

5.3 RECOMMENDATIONS

The South African government should not take for granted the fact that the majority of South Africans are not really concerned with their privacy. Steps should be taken to ensure that privacy within the e-government context is taken seriously as an essential human right issue. These recommendations outlined below have been dealt with to some extent in the Access to Information Act of 2000 and subsequent regulations but it has not gone far enough.

- The South African public should be made aware of their rights to access data and to correct this data if necessary;

- Public service employees should sign a Public Services Trust Charter as part of their employment contract with government;
- The public should be aware of this Charter which should contain a privacy statement and Codes of Practice which will outline for them, how to access their personal data and to correct information errors;
- The Information Officer responsibility (as outlined in the Access to Information Act of 2000) should be extended to ensuring accuracy and reliability of data held within government databanks;
- That a Privacy Commission be set up as a statutory body with the following tasks:
 1. Investigate complaints and assist government departments to routinely comply with privacy rules and legislation;
 2. Educate and inform the public on how to protect their privacy and how to access public information from government;
 3. Provide a privacy hotline where individuals and government departments can get general information and advice concerning their rights under current, future legislation and the constitution;
 4. Conduct policy analysis on proposed and existing legislation for privacy implications;
 5. Conduct ongoing research into the technological and social developments that can affect personal privacy;
 6. Meet with the relevant records management personnel in each government department regularly to identify and address privacy concerns of both government and citizen;

5.4 AREAS FOR FURTHER RESEARCH

There is a need for expansion in many areas touched upon by this research. These areas are identified as:

- Privacy and identity;
- Encryption and the use of technologies to safeguard privacy;

5.5 CONCLUSION

The devil is truly in the data and it is clear that with all the efforts of mice and men, in this particular case, the future of e-government, if the management of data and its implication on the privacy of citizens are not clearly put at the forefront of the agenda, then the future for trust in this new relationship with government will not bode well for its implementation and continued success.

REFERENCES

- Agre, P.E., Rotenberg, M. [Ed]. (1998) *Technology and Privacy: The New Landscape*. MIT Press, Cambridge Massachusetts.
- Baker, P.M.A., Akridge, S., Christensen, J.J., Keck, R. (2002). *Policy perspectives on Government Use of Citizen Data: Balancing Security and Privacy Concern*. OTP Policy Paper Series. April 2002.
- Banks, D., Oxman, J., Rodgers,S., Irish,P. (2002). *Missing in Action: An operational definition of E-Government*. EGOV 0101 Class March 2002. Information Resources Management College, National Defence University. Ft. Leslie J. McNair, Washington DC.
- Blakely, C., Matsuura, J. (2001). *E-Government: Is e-democracy inevitable?* Alliance Law Group LLC. Paper prepared for “Innovations for an e-society. Challenges for Technology Assessment”. Berlin, Germany: Oct 17-19, 2001.
- Bozz, Allen and Hamilton. (2001). *Balanced E-Government: Connecting efficient administration and responsive democracy*. A study by Bertelsmann Foundation. Bertelsmann Stiftung.
- Brin, D. (1998). *The Transparent Society: Will Technology force us to choose between privacy and Freedom?* Perseus Books, Reading Massachusetts.
- Buys, R. [Ed.] (2000). *Cyberlaw: The law of the Internet in South Africa*. Van Schaik.
- Cabinet Office, UK (2002). *Privacy and data sharing: the way forward for public services*. A performance and Innovation Unit Report. April 2002.

Caldow, J. (1997). *Governance in the Information Age*. A White Paper from the Institute for Electronic Government's 2nd Annual Leadership Workshop.

Crossing Bridges. (2002). *The Privacy Challenge – Connecting citizens with all levels of Government*, Conference Board of Canada's 2002 eGovernment Conference, Crossing Bridges to Success, May 9, 2002, Ottawa, Ontario

Department of Information Resources, Austin Texas. (2000). *Privacy Issues involved in Electronic Government*. Prepared for the Electronic Government Task Force: Strategic Issues Sub-Committee. August 2000.

Dinsdale, G., Chhabra, S., Rath-Wilson, J. (2002). *A Toolkit for E-Government: Issues, Impacts and Insights*. Canadian Centre for Management Development, November 6, 2002.

DPSA. (2001). *Electronic Government: The Digital Future – A public Service IT Policy Framework*. Department of Public Service and Administration, Republic of South Africa. February 2001.

DPSA. (2002). *Information Technology Planning Guidelines*. South African Government 2002. Department of Public Service and Administration.

Electronic Communications and Transactions Bill. B8B – 2002. ISBN 0 621 32190 7.

EU Advisory Body on Data Protection and Privacy. (2001). *Recommendation 2/2001 on certain minimum requirements for collecting personal data on-line in the European Union*. Adopted on 17th May 2001. Article 29 – Data Protection Working Party.

Flaherty, D.H. (1989). *Protecting Privacy in Surveillance Societies: the Federal Republic of Germany, Sweden, France, Canada, and the United States*. University of North Carolina Press.

Forman, M. (2002). E-Government Strategy: Simplified Delivery of Services to Citizens. Executive Office of the President, OMB, Washington, DC. February 27th 2002.

Fountain, J.E. (2002). Information, Institutions and Governance: Advancing a basic social science research program for digital government. National Centre for Digital Government. John F. Kennedy School of Government, Harvard University. May 2002.

Garfinkel, J. (2001). Database Nation: The Death of Privacy in the 21st Century. Pub: O'Reilly.

Gavison, R. (1984). Privacy and the limits of law in *Philosophical Dimensions of Privacy: An Anthology*, New York: Cambridge University Press (Schoeman, F., ed).

Gordon, G. (2003). Identity Fraud: Easier detection of irregularities. *Financial Mail* May 2, 2003.

Hart-Teeter. (2003). The New E-Government Equation: Ease, Engagement, Privacy and Protection E2P2. Prepared by Hart-Teeter for the Council for Excellence in Government. Accenture. April 2003.

Jupp, V., Domenech, J. (2001). E-Government: Connecting the dots? Accenture.

Klima, J. (2002). The E-government Act: Promoting e-quality or exaggerating the digital divide?

McClure, D.L. (2000). Electronic Government: Opportunities and Challenges facing the FirstGov Web Gateway. *Information Technology Management Issues*. GAO-01-087T. October 2nd 2000.

McClure, D.L. (2001) *Electronic Government: Challenges must be addressed with Effective Leadership and Management*. United States General Accounting Office. GA)-01-959T. July 11, 2001.

McDermott, P. (2000), What is e-government – How will it affect us?

Mladen, C. (2003). Privacy in Canada. A Report of Research on Privacy for Electronic Government.

Mostert, W. (2003). Electronic Records Management: legal issues. Deloitte & Touche Legal, Sandton, Johannesburg. South Africa. 2003.

Mouton, J. (2001). How to succeed in your Master’s & Doctoral Studies: A South African Guide and Resources Book. Van Schaik.

Mouton, J. (2002). Understanding Social Research. Van Schaik.

Pepper & Rogers. (2002). Role of Personalization and Privacy in Streamlining Government. Peppers & Rogers Group.

Quinlan, Dr. A., Buckley, D., Schon, E., Harris, C. (2001). E-Government: A Submission to the Congressional Internet Caucus Advisory Committee E-Government Task Force by Department of Government, University College, Cork, Republic of Ireland. February 28 2001.

Riley, T.B. (2002). Change Management and E-governance and International Privacy Issues and the Relationship to E-government. Commonwealth Centre for Electronic Governance. London, UK.

Riley, T.B. (2003). Information Management and E-government. International Tracking Survey Report '03. Commonwealth Centre for Electronic Governance. March 7 2003.

Schoeman, F.D. [Ed] (1985). Philosophical Dimensions of Privacy: An Anthology. Cambridge University Press.

Shetty, K.A.V. (2003). Why most e-government projects fail. The Hindu Business Line. Saturday, Nov. 15, 2003.

Smith, M.S. (2002). Internet Privacy: Overview and Pending Legislation. June 20 2002. Congressional Research Service. Library of Congress.

Stiglitz, J.E. Orszag, P.R., Orszag, J.M. (2000). The Role of Government in a Digital Age. Commissioned by The Computer & Communications Industry Association, October 2000.

Tambouris, E., Gorulas, S., Boukis, G. (2002). Investigation of Electronic Government. Archetypos SA, Athens, Greece.

The Commonwealth Centre for Electronic Governance. (2001). Electronic Governance and Electronic Democracy: Living and working in the Connected World. Url: http://www.electronicgov.net/pubs/research_papers/erged.shtml.

The Constitution of the Republic of South Africa, 1996. Act 108 of 1996. Annotated Version. Constitutional Assembly.

The Working Group on E-Government in the Developing World. (2002). Roadmap for E-government in the Developing World: 10 questions e-government leaders should ask themselves. Pacific Council on International Policy.

W’O Okut-Uma, R. (2000). Electronic Governance: Re-inventing Good Governance. Commonwealth Secretariat London. 2000.

Whitaker, J., Hewett, W.G. (2000) Data Protection and Privacy” The Emerging Australian Legislation and its implications for IT Professionals. School of Management Information Systems, Deakin University, Australia. Presented at the Australian Information Management Workshop.

Zahran, Dr.S. (no date). E-government: A strategy for modernizing Governments.
Evaluator for ICT European Community Projects.

