SECURITY, PRIVACY AND ETHICS IN ELECTRONIC RECORDS MANAGEMENT IN THE SOUTH AFRICAN PUBLIC SECTOR

Mpho Ngoepe
Auditor-General of South Africa
Email: MphoN@agsa.co.za

Lebohang Mokoena
National Archives and Records Service of South Africa
Email: Lebohang.Mokoena@dac.gov.za

Patrick Ngulube
University of South Africa, Department of Information Science
Email: ngulup@unisa.ac.za

Received: 9 March 2009
Revised: 5 April 2010
Accepted: 3 May 2010

Abstract

Computers have become such valuable tools for conducting business that today people would have difficulty imagining work without them. One great advantage of the computers is the ease with which a large quantity of data can be analysed, manipulated and shared among people. However, there are a number of compelling security, privacy and ethical dilemmas raised by computer systems. For example, the monitoring of employee e-mails by employers to prevent them from wasting organisation's resources on non-business activities. This article seeks to investigate security, privacy and ethical dilemmas in the electronic records management environment in the South African public sector. In order to draw inferences and recommendations, a survey was conducted on existing national government departments in South Africa. Firstly, findings of the literature review (content analysis) are discussed. Secondly, the results from the survey are analysed and interpreted. The article concludes by arguing that without a proper information security framework and professional code of ethics that embrace electronic records management, government departments could expose themselves to unnecessary financial

Open Rubric

losses due to litigations resulting from invasion of privacy and unethical behaviour, and urges government departments in South Africa to implement Electronic Document and Records Management Systems that are able to capture records in read-only format and generate a non-editable audit trail of all actions to address security dilemmas of electronic records.

Keywords: Ethics, Electronic records management, Government departments, Information security, Privacy, Public sector, South Africa

Introduction

Many people would attest that the computer remains one of the greatest gadgets, credited with revolutionising communication throughout the globe. In fact, the computer has become such an integral part of our daily lives that one wonders how mankind survived without it in the past. However, like other technologies, such as cellular phones, television and radio, the computer can be a double-edged sword. One great advantage of the computer is the ease with which a large quantity of data can be captured, analysed, manipulated and shared amongst people throughout the globe (Covington 1995:31). However, individuals and organisations are facing all sorts of risks and drawbacks as a result of computers. For instance, employers can read private e-mails of their network users to make sure that secret company information is not being disclosed or to ensure that company regulations are being followed. In addition, information technology (IT) professionals are asked to monitor the Web sites visited by the employees and keep logs of them. What violates even the rights of the employees are instances where employers can ask IT professionals to place key loggers on network computers to capture every word the employee types.

Furthermore, the computer can be used to commit crimes and threaten cherished social values. Unprotected electronic records can be hacked by identity thieves or stolen in bulk (Laudon and Laudon 2005:153). For example, in July 2005, about 57,000 patient records on back-up tapes were stolen from a Phoenix-based managed care company (Sharpe 2005). In South Africa, for example, there are a number of cases reported in newspapers about identity theft. In many ways our records are our identity and should be properly protected. Further, third parties can mine electronic records for data to market health products or screen out people as insurance or employment risks (Laudon and Laudon 2005; Lynch 2000). Therefore without sufficient attention to ethics, security and privacy all the virtues of electronic records quickly become vices.

In many ways, technology and the management of records are inseparable concepts. For example, in order for a record to be created, there must be a medium on which the record is captured (e.g. clay tablet, papyrus, paper, microfilm and the sector of a computer disc) (Markham 2006:6). In the past, records management was so simple with the use of typewriters and records could be controlled easily by filing clerks (Laudon and Laudon 2005:522). The copiers and printers introduced more volumes of records and a bigger challenge with regard to the management of records. In a digital world, records management got out of control. Now everyone creates e-mails and stores all types of corporate content in many different versions throughout different types of systems within the organisation. These records can potentially be accessed by large numbers of people and are subject to discovery and regulatory requirements, plus malicious and unintended misuse (Markham 2006:6). As a result, a number of compelling security, privacy and ethical dilemmas are raised in the electronic records environment. Electronic systems now reach into all levels of government, into the workplace, and into private lives to such an extent that even people without access to these systems are affected in significant ways by them. Therefore, new ethical and security issues are necessary to balance the needs and rights of everyone.

In view of the above, this article seeks to investigate security, privacy and ethical dilemmas raised by the management of electronic records management in the South African public sector. In order to draw inferences and make recommendations, a survey was conducted on existing government departments in South Africa.

Justification of the study

The study was prompted by the apparent proliferation of electronic records in most government departments in South Africa. As with paper-based records, these records should be properly secured and managed to ensure that they are not compromised in any way. If government departments fail to do so, they could be faced with serious consequences such as prosecution under a number of legal frameworks, or a loss of money and time. As a result, service delivery could be hampered. Therefore, the researchers felt it necessary to establish in practice how privacy in the electronic records management environment is maintained, how electronic records are secured and whether there is a code of ethics in government departments that embraces electronic records management in South Africa.

The importance of this study is also supported by Ngulube (2000:161) when he stresses that the individual's right to information and the need for records management professionals to maintain privacy and security of records are issues that cannot be left unattended. Records management practitioners face many ethical issues in the conduct of their business such as confidentiality and privacy of information (Ngulube 2000:161). Therefore, there is a need to address these issues, hence the researchers embarked on this study.

Furthermore, Britz and Ackermann (2006:3) and Magi (2008:747) argue that many studies have been undertaken about computer ethics and security, but few deal directly with ethics, security and privacy in electronic records management. For that reason, this study attempts to fill the gap by exploring ethical, security and privacy dilemmas in electronic records management in South Africa. It is hoped that the study will serve as a catalyst for modification and formulation of information security policies, codes of ethics and information privacy policies in the South African public sector.

Flowing from the above background, this paper was guided by the following research questions:

- What ethical, privacy and security dilemmas are raised by the management of electronic records in the South African public sector?
- What are the ethical responsibilities of records management professionals in safeguarding electronic records?
- Are there specific guidelines on ethical, security or privacy issues in the South African public sector?

Literature review

A quick scan of literature shows that much has been written about ethics, privacy and security dilemmas in information systems in general. However, as Britz and Ackermann (2006:3) would attest, very few studies reflect on ethics, privacy and security in the electronic records management environment in the South African context. The literature for this study was reviewed under three sub-topics: ethics, privacy and security in electronic records management. In an attempt to step back and reconsider ethical, privacy and security implications raised by electronic records, this article looks for indications of whether computers have indeed created new ethical dilemmas in records management.

Ethics

Ethics refers to the principles of right and wrong that individuals, acting as free moral agents, use to make choices to guide their behaviour (Cardinali 1995:11; Laudon and Laudon 2005:153). This implies that ethics include moral choices made by individuals in relation to the rest of the community, standards of acceptable behaviour, and rules governing members of a profession. According to Ngulube (2000:161) ethics in the records management environment encompass the commitment of practitioners to the standard that is expected of them. As discussed above, the advent of computers raises ethical issues in the management of electronic records for both individuals and organisations. Therefore, there is a need for records management practitioners to address the question of ethics in the electronic environment.

Covington (1995:32) argues that the “hot issue in computer ethics related to record-keeping changes from year to year”. In the early 1980s, for example, it was game playing (e.g., solitaire, hearts, etc.) versus serious work; in the mid-1980s, account cracking; and since 1990, the misuse of computers as a means of mass communication, for example, through sending of private mails at work or sending company information to outsiders via e-mails. Covington (1995:32) aptly summarized the practice: “Within that broad category, the hottest issue was at first general obnoxiousness and harassment;

then indecency and obscenity; and most recently, improper commercialism".

Researchers such as Britz and Ackermann (2006), Covington (1995), Lynch (2000) and Magi (2008) cite the invasion of privacy, control of and access to information and misuse of data as broad issues relating to unethical behaviour which takes place every day in organisations. For example, insurance company employees can view any client's medical history. Often the files are read as a matter of curiosity rather than official business. There have been cases where confidential file materials have been shared with non-company personnel. After checking a medical history and discovering something unknown to anyone else the next logical action for an unethical employee would be to make the information public.

Almost every day there are newspaper reports of unethical activity relating to recordkeeping. A good example of unethical behaviour in the public sector is the well known missing files in Botswana of the former South African Minister of Health, Manto Tshabalala-Msimang. On 27 August 2007, national newspapers in South Africa reported that Tshabalala-Msimang's court records and health files in Botswana were missing. The information was then sold to newspapers. In this case no culprit was charged and records management professionals both in Botswana and South Africa remained silent. Records management professionals, as the custodian of records created by public institutions are responsible for safeguarding such information and should take action if the safety of records is compromised.

Privacy

Another important ethical issue in electronic records management involves privacy. Privacy is the "claim of individuals to be left alone, free from surveillance or interference from other individuals, organisations, including state" (Laudon and Laudon 2005:159). Privacy has been described in the South African Bill of Rights as (Constitution of South Africa 1996):

> … an individual condition of life characterised by seclusion from the public and publicity. This implies an absence of acquaintance with the individual or his personal affairs.

Stair and Reynolds (2007:698) maintain that privacy is one of the most comprehensive of rights and the most valued by civilized man. In an electronic records management environment, privacy deals with the collection and use or misuse of data. Data is constantly being collected and stored on each of us. This data is often distributed over easily accessed networks and without our knowledge or consent. With today's technology, the right to privacy in records management is a challenging problem. More data and information are produced and used today than ever before. The government is perhaps the largest collector of data. Billions of records exist on citizens. When someone is born, takes certain high school examinations, start working, enrolls at the university, applies for a driver's licence, or gets married, a record is created and stored somewhere in a computer database. A difficult question to answer is, "who owns this information?" Is it the government or individuals whose details are captured? If a public or private organisation spends time and resources to obtain data on people, does the organisation own the data, and can it use the data in any way it desires? Legislation answers these questions to some extent for government departments, but the questions remain unanswered for private organisations (Britz and Ackermann 2006:13). In South Africa, many people have experienced a situation where they receive anonymous calls from insurance companies selling them their (insurance companies) products. One wonders how and where these companies got hold of the contact details.

The right to privacy is one of the fundamental rights enshrined in Chapter Two of the Constitution of the Republic of South Africa. Section 14 of the Constitution spells out that "everyone has a right to privacy". In South Africa, the claim to privacy is further protected by the Protection of Information Act (Act No. 82 of 1982), apartheid legislation which still appears on the statute books. The envisaged Privacy and Data Protection Act is also aimed at protecting individual privacy. Although the right to privacy and the right of access to information seem to be contradictory or opposing each other in nature, the Promotion of Access to Information Act (Act No. 2 of 2000), which promotes and protects the individuals' right to access to information does, however, make provision for refusal of information on the grounds of privacy.

Several organs of state in South Africa have search and seizure powers bestowed upon them by Acts pertaining to their particular areas of jurisdiction and the interception of communications such as snail mail, e-mail and telephone calls (Britz and Ackerman 2006:17). These powers are thus created and regulated by statutes that practically accord certain organs of state the power to invade individuals' right to privacy when deemed lawful to do so. The laws mentioned in Table 1, grant the relevant organ of the state "full and unrestricted access" to any "electronic record or information".

Most likely, problems in respect of private information at the workplace will arise during a search for (and of) such electronically stored records or information. The introduction of technology and electronic communication tools (e-mail and Internet) into the workplace has irreversibly changed the way business is conducted. Nowadays, it is a commonplace occurrence to find private information on computers at the workplace. In the case of search and seizure, this may obviously pose a threat to the employee's right to privacy, but the border between an employee's right to privacy and the interests of an employer is decidedly blurry. The right to privacy in the workplace extends to and protects not only the right to physical privacy, but also the right to privacy in respect of personal data to which the employer may have access as a result of the employment relationship. The issue which requires consideration is the extent to which access to an employee's private information can be gained.

Clearly, the right to privacy is not an absolute right nor is it a paramount value. The right to privacy as provided for in section 14 of the Constitution is however, closely linked with the paramount value of human dignity and exists where there is a reasonable expectation of privacy, the workplace being one such arena. The right to privacy just like other constitutional rights enshrined in the Bill of Rights is not an entirely unfettered right. One must balance employer and employee interests in dealing with the issue, and in determining whether an organ of state has the right to invade this privacy during the course of an investigation. Therefore, an individual's right to claim privacy cannot be used as defence to cover up or condone illicit acts. Notwithstanding the right, where compelling grounds to justify an invasion of the right could be provided an exception akin to lawful search and seizures as contained in sections 19-36 of the Criminal Procedure Act (Act No. 51 of 1977) could be permitted under very stringent rules ensuring that an individual's constitutional right to dignity is as far as possible kept intact (Section 10 of the Constitution, Act No. 200 of 1996).

Table 1 compares the search and seizure powers of the different organs of state in South Africa in relation to violation of privacy.

Table 1: Acts on search and seizure powers

Organ of State	Act of Parliament	Search and seizure power	Procedure
Auditor-General of SA	Public Audit Act, 2004 (Act No. 25 of 2004)	(i) Section 15(1) read with 15(2) empowers the Auditor-General to enter premises of auditee, for purposes of conducting an audit, without a warrant. (ii) Section 16(1) empowers the Auditor-General to enter and search private dwellings and/or persons, which action must be sanctioned by a warrant issued by judge or magistrate. A reasonable suspicion must exist that material is kept or hidden on the premises.	• Auditor-General *ex officio* authorised to enter and search premises of auditee for purpose to conduct audit. • Warrant not a pre-requisite. • Action must be sanctioned by warrant issued by judge or magistrate. • Information in form of affidavit on oath or affirmation to establish reasonable suspicion that material is in possession or under control of a person or on the premises.
Financial Services Board	Inspection of Financial Institutions Act, 1998 (Act No. 80 of 1998)	(i) For purpose of inspection of institution an appointed inspector may at any time enter and search premises occupied by institution. (Searches are limited to premises occupied by the institution). The entry and search of private persons or premises not occupied by an institution is only possible on the authority	• An appointed inspector *ex officio* authorised to enter and search any premises occupied by institution and seize material related to the affairs of the institution. • Warrant may be issued on application by magistrate or judge.

Organ of State	Act of Parliament	Search and seizure power	Procedure
		of a warrant. (ii) An inspector may proceed without a warrant, if a person in control of the premises consents to the entry and search of the premises.	- Information in form of affidavit on oath or affirmation to establish reasonable belief that material related to affairs of institution is kept on premises.
South African Revenue Services	Amendment of Income Tax Act, 1996 (Act No. 46 of 1996)	Section 57D empowers a Commissioner, on application and only when authorised by a warrant, issued by a judge, to enter and search any premises and search any person present on the premises.	- An application to a judge which consists of a Notice of Motion and founding affidavit on oath or solemn declaration to establish reasonable grounds that an offence has been committed or to establish non-compliance of a person's obligations.
Special Investigations Unit	Special Investigating Unit and Special Tribunal Act, 1996 (Act No. 74 of 1996)	(i) A member of the Special Investigation Unit, for purpose of performing functions, under authority of a warrant, issued by a judge or magistrate, may enter and search any premises. (ii) A member of the unit can without a warrant enter and search any premises for material if a competent person consents thereto or if the member believes on	- Warrant may be issued by a judge or magistrate - Information in the form of an affidavit on oath or affirmation to establish reasonable grounds that material is in possession or under control of any person on any premises.

Organ of State	Act of Parliament	Search and seizure power	Procedure
		reasonable grounds that a warrant will be issued on application, but the delay in obtaining a warrant would defeat the object of the search.	
Medicines Control Council	Medicines and Related Substances Control Act, 1965 (Act No. 101 of 1965)	(i) An appointed inspector has very wide powers to enter and search any premises on which describ: bed medicines are present in terms of section 28 of the Act. (ii) A private dwelling can only be entered and searched by an appointed inspector under authority of a warrant.	• Warrant may be issued by magistrate on information on oath or affirmation. • Information before a magistrate in the form of affidavit on oath or affirmation to establish reasonable grounds.
Competition Commission	The Competition Act, 1998 (Act No. 89 of 1998)	(i) Section 47 of the Act provides for entry and search of certain premises without a warrant, if person in control consents or if the inspector has reasonable grounds for believing that a warrant would be granted, but delay in obtaining it would defeat the object of the entry and search.	• Warrant may be issued on application by a magistrate or judge. • Information in form of affidavit on oath or affirmation to establish reasonable grounds that a prohibited practice has taken place.
National Prosecuting Authority	National Prosecuting Authority,1998 (Act No. 32 of	Sections 29(5) read with sections 28(13) and (14) of the Act provide for entry and search of a premises on reasonable suspicion that a specific offence had been commit-	• An Application to judge which consists of Notice of Motion and founding affidavit on oath or affirmation.

Organ of State	Act of Parliament	Search and seizure power	Procedure
	1998)	ted or objects in relation to investigation of specific offence, could be found on the premises.	• Information must establish reasonable suspicion that an offence had been committed, or the object in relation to an offence is possibly on the premises.

Security

Security of records poses another ethical issue raised by the advent of computers. Security refers to the policies, procedures, and technical measures used to prevent unauthorised access, alteration, theft or physical damage to information (Laudon and Laudon 2005:526). There are a number of security dilemmas in electronic records management. There can be illegal access and use of records, data alteration and destruction (Stair and Reynolds 2006: 583). Therefore organisations need to control access to their records, as records contain personal and operational information that should be protected against unauthorised access. Katuu (2004:6) argues that there are numerous protection mechanisms that could be employed to safeguard electronic records such as updating virus software, using firewalls, authenticating access, using security software, etc. Other methods of securing data involve the use of Public Key Infrastructure (PKI) to securely and privately exchange data through the use of a public and private cryptographic key pair. Data can also be encrypted so that if stolen it remains unreadable. Encryption is a technique that converts data into a secret code (Magi 2008:747).

Information security environment in the South African public sector

A crucial facet of the electronic information security regulatory framework in the South African public sector is the influence brought to bear by identified relevant key stakeholders including the Department of Public Service and Administration (DPSA), State Information

Technology Agency (SITA), National Intelligence Agency (NIA), The South African Communications Security Agency (SACSA), Department of Communication and to a large extent the National Archives and Records Service of South Africa (NARSA). This aspect of the discussion will focus on each of the above mentioned role players' contributions in shaping the information security regime in the context of the South African public sector.

It is against the backdrop of a need for a holistic and multidisciplinary approach, that any initiative towards formulating an effective policy framework on information security should acknowledge a number of laws and policies emanating from the strategic stakeholders mentioned above. The Public Service Act of 1994 stipulates that the Ministry of Public Service and Administration is responsible for any policy which relates to information management and information technology in the public service, and the provision of a framework of norms and standards with a view to giving effect to any such policy.

While DPSA has a chief responsibility of implementing an overarching information security policy framework in the public service, this responsibility cannot be smoothly discharged without being cognisant of the cross-cutting roles played by the various critically important role players in the government information security environment. As a result, the Department of Public Service and Administration's Draft Information Security Framework Policy of 2001, does recognise the relevant role players by drawing from their pieces of legislation and policies which impact on information security.

The Draft Information Security Framework has an express purpose of creating "a framework for consultation" starting with the endorsement of international best practice, in particular the ISO 17799, and the consequent "adoption of information security policies from relevant role players as a blue print to inform respective departmental and state organs' internal security policies" (Department of Public Service and Administration 2001:3). The framework would form the basis for policy guidelines targeted among others at:

- fighting cyber crime;
- controlling access to information;
- planning for business continuity;
- complying with legal and policy requirements;

- developing and maintaining in-house software;
- controlling e-transaction information security;
- detecting and responding to information security incidents, to mention but a few aspects; and
- classifying information and data.

A number of laws, regulations, standards and policies produced by the various government role players interested in information security, place governmental bodies under increased pressure to ensure that adequate electronic information security exists in the public sector. Keakopa (2007:70) provides evidence to the effect that South Africa has a well developed statutory and regulatory policy framework to guide public service agencies to manage electronic records management. However, there seems to be no adequate proof to suggest that a sufficient number of government departments have taken advantage of these available overarching policy guidelines through customisation into internal agency specific electronic records management policies and procedures.

In 1996 the South African Cabinet approved the Minimum Information Security Standards (MISS) administered by the National Intelligence Agency, as national information security policy. In terms of the MISS document, the head of an institution in the public sector has a responsibility to create security awareness of personnel using computers. The MISS policy further puts a responsibility on government departments to ensure that all computer storage media are handled according to the document security standards. The policy also requires encryption to be applied for top secret information and a record kept of classified documents transmitted and received.

Another piece of legislation worthy of mentioning is the State Information Security Agency Act (Act No. 88 of 1998) which states that the objective of SITA is to provide information technology, information systems and related services in a maintained information systems security environment to participating departments and organs of state.

In 2002, the Electronic Transactions and Communications Act (Act No. 25 of 2002) was passed to promote e-government services and electronic communications and transactions within public and private bodies, institutions and citizens. The ECT Act also seeks to promote universal access to ICT infrastructure primarily in the under-serviced areas. Nevertheless, with access to information communication technology infrastructure certain technical information security measures such as the implementation of digital signatures, authentication and cryptography have to be observed in terms of the ECT Act to prevent abuse of information systems. Furthermore, the Act stipulates that the Minister of Communication may by notice in the Gazette prescribe matters relating to:

a. the general management of critical databases;
b. access to, and transfer and control of critical databases;
c. infrastructural or procedural rules and requirements for securing the integrity and authenticity of critical data;
d. procedures and technological methods to be used in the storage or archiving critical databases; and
e. disaster recovery plans in the event of loss of critical databases or parts thereof.

By and large, the ECT Act stipulations echo what has already been mentioned above as being the object of laws and policy prescripts from role players such as DPSA and NIA.

The National Archives and Records Service of South Africa, on its part, has a responsibility in terms of section 13(2)(b)(iii) of the National Archives and Records Service Act (No. 43 of 1996) to determine the conditions subject to which electronic records systems shall be managed. According to Kirkwood (2008; par 2.1), the reasoning behind this provision is to ensure that integrated electronic records and document systems are implemented through which records in all formats are managed in an integrated manner, and that such systems provide specified minimum records management functionality. Adequate records management functionality requirements have to be built into electronic records systems to safeguard the reliability and authenticity of records and their legal admissibility, enable them to be retrieved in context, maintained and preserved over time and to facilitate disposal (Kirkwood: 2008:par 2.1).

The NARS Act is also complemented by clearly laid out policy prescripts relating to the regulation of current electronic records systems (otherwise called Enterprise Content Management or ECM systems) that are published on the National Archives website at http://www.national.archives.gov.za under the links to *Services to Governmental Bodies* and *Records Management Publications* in order to assist governmental bodies including agencies in the public sector. The following are examples of available publications which were benchmarked against national and international electronic records management standards:

- *Advisory Pamphlet No 2 – Electronic records and the law: what governmental bodies need to know*
- *Managing electronic records in governmental bodies: policy, principles and requirements*
- *Managing electronic records in governmental bodies: Metadata requirements*

According to Kirkwood (2008) the advent of the Free and Open Source Software policy in the public sector has implications for electronic records systems. In this regard as well, the National Archives and Records Service (NARS) is actively participating with developers of an Open Source Software product being piloted by the Department of Science and Technology to ensure that records management functionality requirements are incorporated as determined by the NARS.

It is worth delving into different aspects of information security that may be addressed in the electronic records management content, namely physical security, content security, network security and personnel security.

Physical security

For instance, the need for provision of physical security relates to the infrastructure that houses the information. In the cyber/electronic environment, this refers to computer hardware, servers, mainframes, systems and other end user gadgets and devices. Such kinds of security can be optimally provided for in the public service by the respective organisations through the implementation of internal security arrangements and measures with reference to government-wide specific guidelines.

Content security

Secondly, an aspect of information security concerned with protection of content cannot be fully covered in the electronic environment through merely addressing physical security since in the electronic records realm, tangibility, physical location, time and distance become irrelevant. Hence, content security is provided for by way of, for example, firewalls, passwords, access codes, biometrics cryptography and encryption. The security measures provided for content can be varied with differing levels of sophistication depending on the sensitivity and secrecy of the information.

Network security should be provided for information in transit including transfer protocols, applications, switches and routers. To supplement what is provided for in content security, network security measures provide for Public Key Infrastructure and certification to ensure authenticity, integrity, confidentiality and non-repudiation of communications, messages, transactions or information in transit.

Personnel security

Lastly and arguably most importantly, is the necessity of addressing personnel security, which focuses more on the security of individuals who deal with sensitive and top secret information. This area of information security has a bearing on the notion of addressing ethical questions, as employees such records managers and other staff members who wield discretionary powers regarding ensuring public access to security classified information have to be subjected to integrity testing processes and provided with an ethical code of conduct that should set parameters within which they must operate.

While digital signatures and encryption may address information security concerns, some national archives authorities around the globe do not accept electronic archival records with digital signatures and encryption. For example, the Library and Archives Canada (LAC) considers encryption to serve the function of a traditional paper envelope: Because this “envelope” is not an integral part of the document, and because envelopes have not traditionally been appraised as having archival value, the LAC does not preserve the encrypted version of records in electronic form. For digital signatures, LAC have chosen not to maintain the capacity to re-verify a digital signature after the records are transferred to LAC’s control, or to preserve the traces of a digital signature generated under the Government of Canada Public Key Infrastructure system. LAC considers that the integrity and authenticity of electronic records will continue to be inferred from their placement within an organisation’s record-keeping system during the normal course of business, and from proof of that organisation’s reliance on records kept within their record-keeping system.

Scope and methodology

This study was limited to 37 South African national government departments which were listed on the government website http://www.info.gov.za/aboutgovt/dept.htm. Statutory bodies, municipalities and provincial government departments, even though they form part of the spheres of government in South Africa were excluded from the study. Private sector organisations were also excluded. The study focused only on ethical, privacy and security dilemmas in electronic records management.

In order to assess the security, ethical and privacy dilemmas in South Africa, this study used questionnaires directed at either records managers or chief information officers of all national government departments for primary data collection. The data upon which studies of this nature is based are often very sensitive (Magi 2008:755). Therefore, a website link to the questionnaire which allows anonymity was created and sent to all the respondents. All the participants were given seven days or less to complete the questionnaire online. Similar research carried out elsewhere by researchers such as Cottrell (1999), Kritzinger (2006), Magi (2008), Ngulube (2000) and Sturges *et al*., (2003) used a questionnaire as the main instrument for data collection.

Discussion of the findings

Starting with the response rate and the profiles of the respondents, this section discusses the major findings of the study. The aim of the survey was to investigate ethical, privacy and security dilemmas raised by the management of electronic records in the South African public sector.

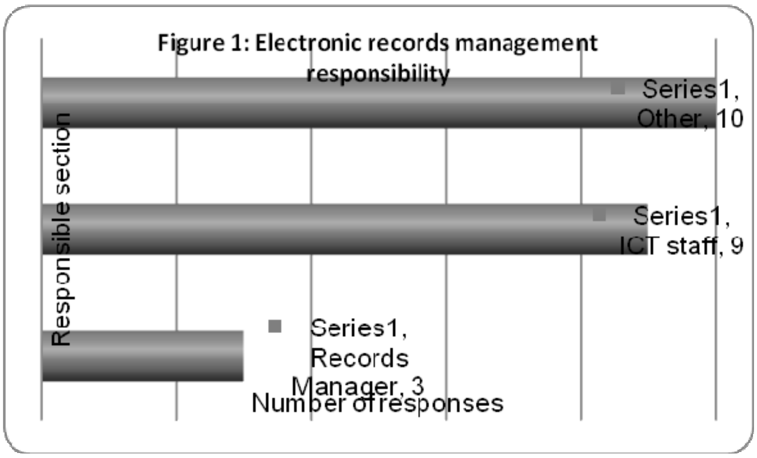
Response rate

The initial response rate for this study was poor with only six completed questionnaires out of possible 37 being returned. This prompted the researchers to contact the respondents telephonically to solicit information. It was established that most respondents were under the impression that the survey would be used as a monitoring or evaluation tool to check their compliance with legislation, as well as to test their knowledge on ethics, security and privacy issues. After a lot of follow-ups and persuasion, as well as explaining the purpose of the study to the respondents, 15 more respondents returned the completed questionnaires electronically taking the tally to 22, thus representing a 59% return rate. The analysis was done based on the assumption that a response rate of over 50% is considered a safe number to detect a pattern (Babbie and Mouton 1998:261). Questionnaires were captured and analysed through an open source survey tool.

Participants' profile

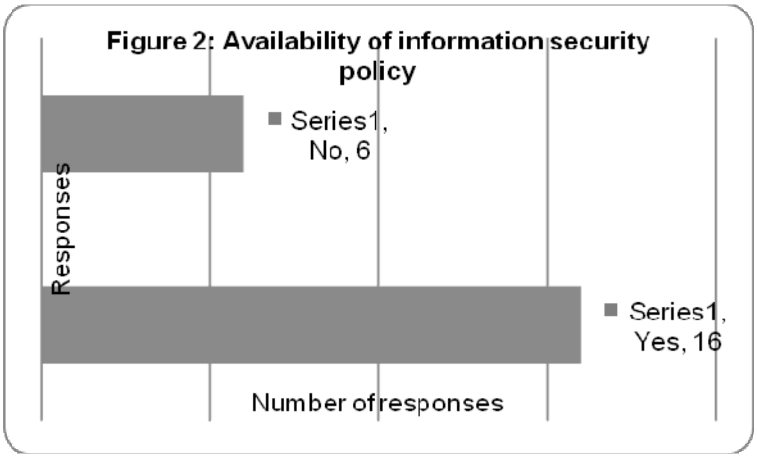
Of 22 participants who returned questionnaires, 31.8% (7) were females as compared to 68.1% (15) of males. Eight (36.4%) of the respondents had a bachelors degree as compared to 22.7% (5) with a diploma. Only 6 of the respondents with degrees and diplomas had qualifications in archival and records management studies (postgraduate diploma or national diploma). A further 40.9% (9) cited other postgraduate qualifications such as MBA, PhD in History and MSc in Computer Science.

Of the 22 participants, 40.9% (9) were records managers, 9.1% (2) were information technology managers, 9% (2) were senior managers in records management whereas 18% (4) were Chief Information Officers. The other 22.7% (5) were on assistant director level. As indicated in Figure 1, only 13.6% (3) of the respondents indicated that the responsibility of electronic records management resorted with the records manager, as compared to 40.91% (9) that indicated that it was the responsibility of the ICT staff. The other 45.5% (10) indicated that electronic records management was a shared responsibility between the ICT unit and records management unit, with the records management unit being the custodian and providing the specifications for records systems while the ICT unit provided the tools.



Security issues in electronic records management

Participants were asked to state or indicate whether their departments had an information security policy. As shown in Figure 2, only 27.3% (6) did not have a policy as compared to 72.7% (16) that had a policy. Of those 16 with a policy, only nine indicated that the policy was endorsed by the head of department and communicated to all staff members. The other seven indicated that the policy was still at a draft stage. The dates when the policies were last reviewed as indicated by the participants, varied from 2003 to 2008. The departments without the policy indicated that information security was incorporated in other policies such as the ICT policy, records management policy and e-mail policy.



When asked how their departments secured electronic records from unauthorised access and tampering; as well as how they ensured the integrity and authenticity of electronic records, four participants indicated that access to records systems was controlled with user IDs and encrypted passwords. Three indicated that an audit trail was kept on all objects records in the Enterprise Content Management (ECM) and it kept check of all changes made to the objects. The ECM allows for certain system generated metadata fields to be captured and in conjunction with the audit trail kept in the system, authenticity can be ensured. Two captured metadata that controls access to records. In this regard, access to records was role based, meaning that employees did not have access to records for which they were not allocated rights. Two others indicated that objects received via e-mails on platforms such as JPG and video clips were quarantined in order to prevent viruses from entering their systems. However, quarantined e-mails could be released for access by the intended recipients if the employee could justify to the IT security manager that it is business related. Two departments indicated the usage of firewalls and digital signatures as the security measure.

Only one participant indicated that his/her department ensured the authenticity and integrity of electronic records by observing the minimum required metadata and audit trails as set by the National Archives and Records Service of South Africa. The department was using an Integrated Document and Records Management System (IDRMS) that was able to capture records in read only format and a non-editable audit trail of all actions to be placed on a record. The business rules embedded in the IDRMS allocate different rights to different user groups, for example some employees have only the right to view without being able to edit. Only the administrator has the right to delete records. Other government departments used electronic signatures. However, 36.3% (8) of the participants indicated that no specific measures were used for unstructured records, although version control was used in certain instances. In structured databases specific controls and validations are normally built into systems to ensure authenticity.

Participants were asked to state whether electronic records were ever tampered with in their departments. Only one participant indicated that electronic records were once tampered with in his/her department. Apparently, in 2006 the IT manager in that particular department deleted a case file on the system. Upon investigations, the audit trail revealed the culprit; as a result the official was suspended and subsequently discharged from his duties. One other participant indicated that an offensive e-mail was once sent from an employee's e-mail account to all staff members. Upon investigation it was found that the employee left his computer unlocked and the possibility of colleagues playing pranks could not be ruled out.

When asked what security challenges the government departments experienced, most participants indicated that security is dependent on user compliance to policies and procedures, and it was therefore not always possible to ensure that records were managed as securely as they should be. The biggest issue was that users did not comply with security policies. Other respondents cited the challenges for the management of e-mails, as well as the records that users saved on the hard drives. One respondent indicated that "electronic records are viewed differently to hard copy records – it is not always seen as "official" records with the same "value" as hard copy records. Because of the way it is generated, e.g. by a user sitting behind his/her own PC, it is not seen as something belonging to the department. It is therefore a lot easier to simply delete or "give" it to somebody else. Users seem to think that different rules, if any, apply to it".

Ethical issues in electronic records management

Participants were asked to indicate whether departments had a documented code of ethics that embraces electronic records. As shown in Figure 3, only 13.6% (3) of government departments had a documented code of ethics, as compared to 86.4% (19) which did not have one. All government departments with a documented code of ethics indicated that users did not adhere to the code. Some of the departments without a code of ethics indicated that issues of good conduct by employees were addressed in employment contracts.

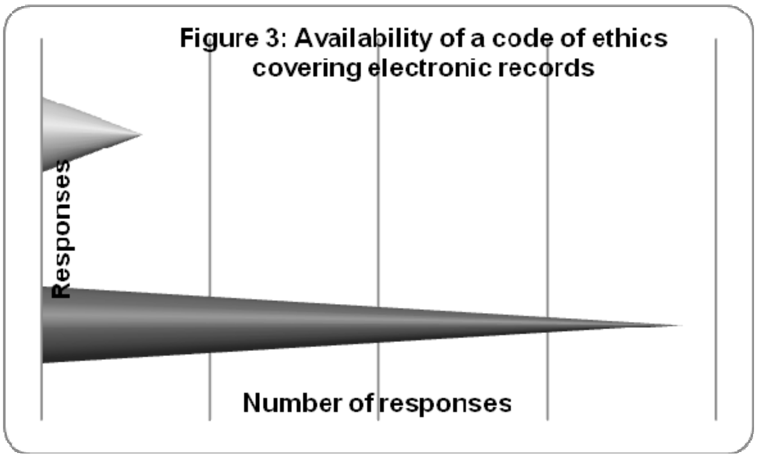


Figure 3: Availability of a code of ethics covering electronic records

The ethical issues regarding electronic records management as cited by the participants include the following: the monitoring of e-mails through the means of Minesweeper (application for filtering e-mails) by government departments; and forwarding of high capacity e-mails to everyone in the organisation. One respondent cited an example of an employee who received a 3MB e-mail from one of his friends and decided it was a good idea to share it with the rest of the organisation. This resulted in the organisation's email servers crashing with the onslaught of traffic. Clearly many employees were rather unimpressed at the massive mail hitting their boxes and to add insult to injury each one of these disgruntled users had to let everyone else know that they were not happy at all and so hit the "reply to all" option in Microsoft Office Outlook, opting for their names to be removed from the distribution list. However, what they did not seem to realise was that each time one of them replied to all, they sent the same mail back through the server again. One can imagine the chaos that IT had to deal with, as the servers were sending the same e-mail backwards and forwards.

Privacy issues in electronic records management

Participants were asked to indicate whether their departments had a privacy policy that embraces electronic records. As indicated in Figure 4, 63.6% (14) of government departments had a policy which was approved by the head of department, as compared to 36.3% (8) which did not have. Those who did not have a policy indicated that the IT security policy had clauses on privacy, but there was no specific policy that dealt with privacy per se. Others indicated that the policy was part of a disclaimer on the e-mail signature. Others indicated that the e-mail and internet policies also embraced the issue of privacy in the electronic environment. One participant even mentioned that when employees access the internet icon in the departmental computer, terms and conditions appear on the screen and the employee should accept them before he/she could access the internet. These terms and conditions address issues of privacy and deter employees from visiting offensive websites. However, the participant indicated that employees had a tendency of accepting terms and conditions without reading or understanding them.

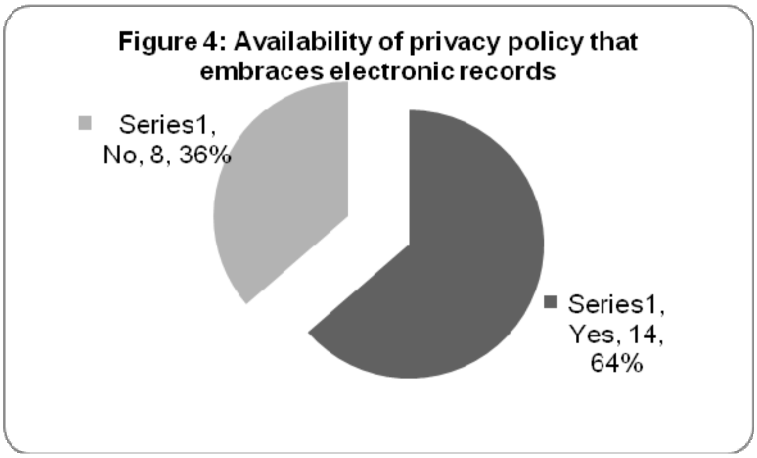


Figure 4: Availability of privacy policy that embraces electronic records

Participants were also asked to indicate whether e-mails were monitored in government departments. The majority, that is 72.7% (16) of government departments monitored employee e-mails as compared to 22.7% (5) which did not monitor employees' e-mails. Only 4.5% (1) indicated that e-mails were monitored only on special investigations or on request if illegal activities were suspected.

Lastly, the participants were asked to indicate how they rated a given statement on a Likert scale with 6 options. The results are illustrated in Table 2.

Table 2: Summary of the findings

Statement	Strongly Agree	Agree	Undecided	Strongly Disagree	Disagree
We have procedures for resolving privacy issues	-	13(59.09%)	2(9.09%)	4(18.18%)	3(13.64%)
Policies regulating privacy issues are adequate	-	9(40.91%)	1(4.55%)	9(40.91%)	3(13.64%)
We have procedures for resolving ethical issues	-	6(27.27%)	2(9.09%)	11(50.00%)	3(13.64%)
Policies regulating ethical issues are adequate	-	5(22.73%)	1(4.55%)	13(59.09%)	3(13.64%)
Policies regulating confidentiality issues are adequate	-	10(45.45%)	1(4.55%)	8(36.36%)	3(13.64%)
We have procedures for resolving issues of confidentiality	-	13(59.09)	1(4.55%)	4(18.18%)	4(18.18%)
I understand the legal issues that govern the management of government information	1(4.55%)	16(72.73%)	2(9.09%)	2(9.09%)	1(4.55%)
I am aware of the relevant legislation	2(9.09%)	15(68.18%)	3(13.64%)	2(9.09%)	0(0.00%)

relevant to privacy					
I understand the ethical issues that govern the management of government information	1(4.55%)	11(50.00%)	4(18.18%)	6(27.27%)	0(0.00%)
My current job description makes reference to ethics-based responsibilities	1(4.55%)	5(22.73%)	2(9.09%)	11(50.00%)	3(13.64%)
Ethics-based expectations are communicated regularly in my organisation	-	4(18.18%)	2(9.09%)	14(63.64%)	2(9.09%)

In view of the above data analysis, the findings of this study are summarised as follows:

- Most government departments (16) had developed information security policies. However, they tend to take their time to review their information security policies. Even those which did not have policies had made provision in some way, for example by incorporating information security issues in other policies such as e-mails policy, records management policy, etc. According to Lin, Ramaiah and Wal (2003:117) information technologies become obsolete within 18 months. This is true because very often records created and maintained by one generation of software and hardware cannot be accessed by later generations, or, if they can, the records' original structure and the associated contextual metadata cannot be read, for example nowadays almost no computers can read floppy disks. Considering the rapid changes in computer technology it is necessary for the government departments to review their information security policies regularly (at least once a year).

- It seemed most government departments were not managing records according to guidelines on electronic records management issued by the National Archives and Records Service of South Africa, as only one participant made reference to the guidelines. Perhaps this is due to the fact that IT officials are taking the lead in the management of electronic records in government departments.
- As mentioned above, IT units in government departments are taking the lead with regard to the management of electronic records. Perhaps this is due to the lack of IT skills on the part of records management professionals.
- There is a lack of documented code of ethics that embrace electronic records let alone paper-based records in government departments. Almost all respondents (19) indicated that their departments did not have a code of ethics that embraced electronic records.
- The management of e-mails as records is still a challenge in government departments.
- In most instances the privacy of employees in government departments is violated, for example 16 participants indicated that their departments were monitoring employees' e-mails.
- Ethical, privacy and security issues raised by electronic records management include inter alia the following:
    - Forwarding of private e-mails to the global group within the government departments.
    - Deleting of electronic records at users' discretion.

Conclusion and recommendations

This study was able to answer only the following two research questions posed in the introduction:

- What ethical, privacy and security dilemmas are raised by management of electronic records in the South African public sector?

- Are there specific guidelines for conduct that are used to provide guidance about ethical, security or privacy challenges in the South African public sector?

However, the study failed to answer the research question on the *ethical responsibilities of records management professionals in safeguarding electronic records*. This can be attributed to the fact that the participants indicated that ethics-based expectations are not communicated effectively in their departments. Furthermore, their job profiles do not make reference to ethics based responsibilities. Therefore they do not see it as their responsibility to be involved in codes of ethics.

Due to the ethical, privacy and security challenges posed by electronic records as stated above, special guidelines are required for their management. It is all very well for government departments in having an e-mail policy, information security policy and code of ethics which new employees have to sign when they join the department. Without a proper information security framework and professional code of ethics that embrace electronic records management, government departments could expose themselves to unnecessary financial losses due to litigations resulting from invasion of privacy, unethical behaviour and hacking of records systems. Compliance with these policies should be enforced. Government departments cannot be safe if information security policies are not complied with.

This article also calls for the administrators of records in government departments to be knowledgeable in electronic records management and information technology, in addition to their professional training. This will reduce the ICT directorates' leading role in government departments to one of just providing the architecture based on the specifications provided by the users and the records management professionals. As a result, records management professionals will be able to participate in the planning of all new electronic systems and in major modifications to existing systems. Further, they will be able to ensure that electronic records are protected against unauthorised access and ensure that metadata schema are designed.

For security purpose, when electronic records are destroyed, digital shredding technology should be applied to ensure that destroyed records could never be recovered. Finally, government departments are urged to implement an IDRMS that is able to capture records in read-only format and generate a non-editable audit trail of all actions to address security dilemmas of electronic records.

References

Babbie, E. and Mouton, J. 1998. *The practice of social research*. Cape Town: Oxford University Press.

Britz, H. and Ackermann, M. 2006. *Information, ethics and the law.* 1st ed. Pretoria: Van Schaik.

Cardinali, R. 1995. Reinforcing our moral vision: examining the relationship between unethical behaviour and computer crime. *Work Study* 44(8): 11-17.

Constitution of South Africa. 1996. Bill of rights. [Online]. Available WWW: http://www.constitutionalcourt.org.za/site/constitution/english-web/ch2.html (Accessed 9 June 2009).

Cottrell, J. R. 1999. Ethics in an age of changing technology: familiar territory or new frontiers? *Library Hi Tech* 17(1): 107-113.

Covington, M. A. 1995. Design and implementation of a campus computer ethics policy. *Internet Research: Electronic Networking Applications and Policy* 5(4): 31-41.

Department of Correctional Services (undated document). Minimum Information Security Standards (MISS) 1996. [Online]. Available WWW: http://dcs.gov.za/organisation/miss.htm (Accessed 6 January 2009).

Department of Public Service and Administration. 2001. Draft Position Paper on Information Security presented by the DPSA [Online]. Available WWW: http://www.dpsa.gov.za/documents/acts&regulations/frameworks/ecommerce/POSITION%PAPER%20ON%20INFORMATION (Accessed 10 December 2008).

Department of Public Service and Administration. 2002. Amendment of the Public Service Regulations, 2001.Government Gazette Notice No. 23992 vol. 449 of 1 November 2002. Pretoria: DPSA.

Department of Public Service and Administration. 2008. Presentation on e-policy framework. 10 November 2008. Pretoria: DPSA.

Etsebeth, V. 2009. Legal implications of information security governance. [Online]. Available WWW:

http://www.//hdl.handle.net/10210/1837 (Accessed 6 January 2009).

Katuu, S. 2004. Are we information providers or the information police? The uneasy marriage between access and security. Paper read at Access Information Management Services' Annual Records Management Conference in Kruger National Park, SA, 18-21 May 2004.

Keakopa, S. M. 2007. Policies and procedures for the management of electronic records in Botswana, Namibia and South Africa. *ESARBICA Journal* 26: 70-82.

Kirkwood, C. 2008. Inputs given on behalf of the National Archives and Records Service of South Africa to the consultative meeting on policy for the legal deposit of electronic material on 10 March 2008.

Krause, M. and Tipton, H. F. 1996. *Information security management*. Boston: Auerbach.

Kritzinger, E. 2006. An information security retrieval and awareness model for industry. PhD Thesis. Pretoria: University of South Africa.

Laudon K. C. and Laudon J. P. 2005. *Essentials of management information Systems: managing the digital firm.* 6th ed. New Jersey: Pearson Education.

Lin, L. S., Ramaiah, C. K & Wal, P. K. 2003. Problems in the preservation of electronic records. *Library Review* 52 (3): 117-125.

Lynch, M. 2000. Ethical issues in electronic information systems. [Online]. Available WWW: http://www.colorado.edu/geography/gcraft/notes/ethics/ethics.html (Accessed 2 December 2008).

Magi, T. 2008. A study of US library directors' confidence and practice patron confidentiality. *Library Management* 29(8/9): 746-756.

Markham, R. 2006. Retention management: the holy grail of records management. [Online]. Available WWW:www.forrester.com/rb/search/results.jsp?SortType=Date&dAg=10000&N=50179+133001+140946 (Accessed 30 November 2008).

Ministry of Intelligence, 2004. The Comsec Security Audit Regulations Government Gazette Notice No. 26914 vol. 472 of 20 October 2004.

National Archives and Records Service of South Africa, 2006. *Managing Electronic Records Metadata Requirements.* [Online]. Available WWW: http://www.national.archives.gov.za/rms/NARS_DMLIB-4915-v1-NARS_DMLIB (Accessed 13 December 2008).

National Archives and Records Service of South Africa. 2007. *Records Management Policy Management Manual,* October 2007. [Online]. Available WWW: http://www.national.archives.gov.za/rms/pdf (Accessed 12 January 2009).National Archives and Records Service of South Africa, April 2007.

National Archives and Records Service of South Africa. 2007. *Advisory Pamphlet No 1 - Managing public records and the law: what governmental bodies need to know.* [Online]. Available WWW: http://www.national.archives.gov.za/rms/NARS (Accessed 13 December 2008).

Ngulube, P. 2000. Professionalism and ethics in records management in the public sector in Zimbabwe. *Records Management Journal* 10(3): 161-173.

South Africa. 1996. *National Archives and Records Service Act (Act No. 45 of 1996)*.

Stair, R. and Reynolds, G. 2006. *Principles of information systems*. 7th ed. Boston: Thomson.

Sharpe, V. 2005. Perspective: Privacy and Security for Electronic Health Records. [Online]. Available WWW: http://www.medscape.com/viewarticle/517403 (Accessed 2 December 2008).

Sturges, P., Davies, E., Dearnley, J., Iliffe, U., Oppenheim, C. and Hardy, R. 2003. User privacy in the digital library environment: an investigation of policies and preparedness. *Library Management* 24 (1/2): 44-50.