AUTOMATED ACCESS TO INFORMATION FOR CRIME REDUCTION

George Motlhabane

A research report submitted to the Faculty of Management, University of the Witwatersrand, in partial fulfillment of the requirements for the degree of Master of Management (in the field of Information Communications technology, Policy and Regulation)

December 2011

Abstract

This research investigates the role of policy on crime reduction by establishing whether it is inhibiting or enabling e-governance. e-Governance is necessary to automate access by the Department of South African Police Services (SAPS) to information held by the Department of Home Affairs (DoHA). Automated Access to information is needed by SAPS to enhance the identification of perpetrators as a strategy for crime reduction.

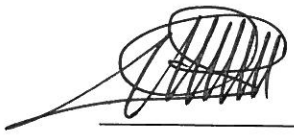
The study explored this process through a qualitative data collection and analysis methodology that utilized a case study of both departments to understand their policy practices with regards to access by SAPS, to information held by DoHA.

The findings revealed that even though the departments are mostly in compliance with access to information policy, this does not enable SAPS to effectively address crime reduction. It was further revealed that the e-governance policy has not been regularly evaluated and adapted to the current identification needs of other departments and has therefore resulted in e-governance not being implemented to enable automated access by SAPS to information held by DoHA.

Access to information and e-governance policies should be modified and adapted to identify emergency departments to take the urgency of their identification requests into account while the perceived benefits of e-governance being developed at DoHA should also be viewed in terms of the benefits to the rest of the departments taking into account their urgency levels.

Declaration

I declare that this report is my own, unaided work. It is submitted in partial fulfillment of the requirements of the degree of Master of Management (in the field of Public and Development Management) in the University of the Witwatersrand, Johannesburg. It has not been submitted before for any degree or examination in any other University.



George Motlhabane

15 December 2011

Dedication

I dedicate the work to my family for all the patience, support, understanding, encouragement and love right through from the beginning to the end of this research report.

Acknowledgements

I would like to thank God for providing me the strength and commitment as well as my wife and the entire family for their patience and support to complete this research report.

I would also like to take this opportunity to sincerely thank my supervisor Lucienne Abrahams whose guidance and continued patience when at times I thought it was impossible, and her relentless push through her "never give up" attitude has assisted me to stay on course throughout the research report process up to completion. She provided extra hours over weekends and after hour sessions of her valuable time that really made it possible for me to achieve the completion of this report.

My appreciation also goes to various other personnel that positively contributed in one way or the other towards the completion of this report. The list includes but is not limited to Simon White, Charley Lewis, Allison Gillwald, Mbombo Maleka and Seth Buhigiro as well as Herman Mashiane, who introduced and literally pushed me to register for this course.

Contents

List of Abbreviations

AFIS……Automated Fingerprint Identification System

ATM…….Automated Teller Machine

B2G……. Business-to-Government

C2G……..Citizen-to-Government

CAS……..Crime Administration System

DoHA……Department of Home Affairs

e-Natis……..Electronic National Traffic Information System

EAI……...Enterprise Application Integration

HANIS…….Home Affairs National Information System

GIP……. Government Information Project

G2B…….Government-to-Business

G2C…….Government-to-Citizens

G2G…….Government-to-Government

ISAD……Information Society and Development

PKC……..Public Key Cryptosystem

MD5A……..MD5 Algorithm

MISS……Minimum Information Security Standards

MIOS……...Minimum Interoperability Standards

MPCC……..Multipurpose Community Centers

NITF……National Information Technology Forum

NPR…….National Population Registry

PNC-ISAD……..Presidential National Commission

ISAD……Information Society and Development

RDP…….Reconstruction and Development Program

SAPS……South African Police Services

List of Tables

List of Figures

CHAPTER ONE: THE IMPACT OF POLICY ON CRIME REDUCTION

1.1 Policy and e-governance challenges for crime reduction

South African government departments perform their administration and manage their databases separately from one another even though there are situations that require departments to cooperate with each other to share information. This access by a department to information held by another department has become necessary for government to fulfill its service mandate. This process is supported by information policy that promotes access to information between departments. Since this raises security and privacy concerns, access to information policy therefore also calls for information to be protected to only allow legal access to information held by government.

The South African Police Services (SAPS) requires access to information held by the Department of Home Affairs (DoHA) to identify perpetrators and reduce crime. The need for this process arises during crime prevention and combating operations when the police need to identify suspects or perpetrators who have never been convicted and do not have criminal records to reflect in the police databases. DoHA, as the only department that is in possession of national civic database, is well suited to assist the police with the personal identification details of all suspects.

Even though access to information policy calls for information held by government to be protected so that everyone's privacy rights should be protected, the policy allows personal information held by the state to be disclosed to third parties for the protection of other rights. It is for this reason that DoHA allows access by SAPS to information in its possession to protect the safety rights of citizens as this process enables the police to identify and apprehending perpetrators of crime.

SAPS and DoHA have implemented e-governance programs, the Automated Fingerprint Identification System (AFIS) and the Home Affairs National Identification System (HANIS) respectively. The departments are utilizing these systems which have automated their fingerprint processing that include rapid identification of all convicted perpetrators of crimes and all citizens by SAPS and DoHA respectively. It should be noted that while SAPS can only store personal

information in the form of criminal records, DoHA stores the personal information of all citizens and visitors. Despite the implementation of e-governance by both departments, the current process of access by SAPS, to information held by DoHA is still manual in some cases and slow. This results in the feedback information from DoHA being mostly late to reach the police in time within the detention deadline to enable them to identify and take appropriate action against the suspects. This is because the police have to take reasonable measure to charge the suspects within the deadline of the detention period as set down in the Criminal procedure act. According to this act, reasonable measures must be taken by the police to charge suspect or perpetrators of crimes within 48 working court hours after detaining them.

Since the police may mostly apprehend individuals on suspicions of various factors including but not limited to stolen identity crimes and hence using fake documents or impersonating their crime victims, the manual access to information at DoHA tends to undermine the operations of the police. This is because the police have to release suspects by the set deadline if they cannot positively identify them, authenticate their fake identity documents through their fingerprints within the deadline.

Even though policy and e-governance that is implemented at both SAPS and DoHA enable access by SAPS, to information held by DoHA, e-governance is not implemented to automate access by SAPS, to information held by DoHA even though this is needed to enhance crime reduction.

The increase in levels of crime and the potential reduction of crime which can be achieved through the automation of access by SAPS, to information held by DoHA, serves as the reason for the selection of SAPS and DoHA as case studies for this research. Should the findings reveal policy as a barrier, the researcher hopes to identify alternative ways and present recommendations for an effective e-governance policy that would create an enabling environment for the implementation of e-governance which is needed to enhance crime reduction operations.

1.2 Background to Crime, political landscape and e-governance

Like elsewhere globally, South Africa is faced by high crime levels that threaten the safety of citizens. The police are continually making efforts to reduce crime where access by SAPS, to information held by DoHA for the identification of the perpetrators of crime has become one of the important processes. The Constitution guides the formulation of policies and their enactment into laws that ensure that only legal access by SAPS, to information held by DoHA takes place. Even though government in general and the two departments have implemented e-governance that is utilized to automate their internal access to information and the identification processes, access by SAPS, to information held by DoHA is manual, slow and mostly yielding inaccurate information. This does not longer assist SAPS to achieve effective crime reduction through perpetrator identification.

1.2.1 Analysis of the crime situation in South Africa

South Africa has a high rate of crime which seems to be higher than most countries. According to local and global media reports on a daily bases one sees front page stories of newspapers and breaking news on television channels reporting assaults, vehicle hijackings, house breaking, murders, rapes, heists of cash in transit vehicle, automated teller machines (ATM) bombings *etc*.

SAPS' annual crime statistics report is based on reported cases registered with the police and contains extensive and comprehensive crime occurrence figures (SAPS, 2010). This report categorizes all incidents of reported crimes by type and period and some summaries will be highlighted hereunder.

The report reveals a steady decrease in crime for the first time since the financial year 1995/1996 up to the end of 2009/2010 financial year during which murder figures dropped to below 17,000 which is the number of reported cases. Even though this figure is still comparatively high, the significant reduction in the murder cases represents a drop of fifty percent (50%) in the murder ratios (SAPS, 2010). The report categorizes the national crime into contact, contact related, property related

and other serious crimes as well as crimes detected as the results of police actions. The percentage categories of these crimes are illustrated in table 1.1 above.

Table 1 1: The national crime category percentages of total national crime

NATIONAL CRIME CATEGORY	PROPORTION OF TOTAL NATIONAL CRIME
Contact crime	31.9%
Contact related crime	6.5%
Property related crimes	26.1%
Other Serious crimes	25.5%
Crimes detected as result of police actions	10.0%

Source: *SAPS, 2010*

Contact crime can be divided further into the categories that are illustrated in table 1.2 above.

Table 1 2: The Proportionate Percentage of Categories of Contact Crime

CONTACT CRIME CATEGORY	PROPORTION OF TOTAL CONTACT CRIME
Murder	2.5%
Attempted murder	2.6%
Assault GBH	30.3%
Common assault	29.2%
Aggravated robbery	16.8
Common robbery	8.5%
Sexual offences	10.1%

Source: *SAPS, 2010*

Contact crime poses a more safety threat to South Africans in general and can be further subdivided into social contact crime and robbery. Social contact crime takes place mainly between people who know one another where violence mostly leads to murder or assault. According to SAPS (2010), murder has dropped by 8.6%

from the 2008/2009 to 2009/2010 financial years. Various other crimes like robbery, assault GBH and common assault are common and committed at random. Assault GBH and common assault constitute sixty percent of social contact crime and according to the stats report, this category of crime experienced marginal increase of 0.5% respectively. SAPS have experienced difficulties in trying to meet the crime operations percentage of between 7% to 10% with regards to assault GBH and common assault due to the fact that, as social crime category, the crime actions do not take place at areas where police can easily detect.

SAPS further explains that the robbery with aggravating circumstances crime category is divided into subcategories of carjacking, truck hijacking, robbery at residential premises (house robbery), robbery at non-residential premises (business robbery), cash in transit (CIT) robbery, bank robbery and Street robberies (which are other aggravated robberies that are not included in the SAPS stats report even though these are aggravated robberies that are being committed in the streets and in other public open spaces).

Even though the number of the subcategories of robberies with aggravating circumstances of cases reported increased while some decreased between the financial years 2008/2009 and 2009/2010, the total number of all subcategory cases that were reported has decreased. According to SAPS the total of all cases decreased by 6.3% which is equal to 7,637 cases calculated from 121 392 to 113 755.

It looks like the South African streets are the most unsafe areas in the country as the stats reveal that even though this subcategory of crime underwent significant decrease and surpassed the maximum reduction target, of 10% by a decrease of 10.4% that yielded the difference of 0.4% between 2008/2009 and 2009/2010 financial years, the number of cases reported is the highest compared to other subcategories standing at 56.9% of all robberies with aggravating circumstances for the financial year 2009/2010. This category's decrease for the period between the financial years 2004/2005 and 2009/2010 financial years amounted to a 38.8% which is 41,020 of case number where carjacking decreased by 6.8%.

1.2.1.2 Crime detected as the results of police action.

The changes in the figures of the cases of crimes detected as the results of police action convey little or no trend messages to the analysts. This is because, as the SAPS stats report indicate, that the increase in the number of cases that are recorded by the police for one of its subcategories for instance, the illegal possession of firearm does not necessarily mean that the number of criminals or the crime level in the area concerned is increasing. This might also mean that while this crime figures remained constant, the police have upped and improved or changed their usual operations and efforts of combating crime.

The new police operations could mean not only the mounting of more road blocks or intelligence driven cordon and search operations, but also having adopted different methods or started operating at unusual places or times of day and thereby catching the criminals off guard and recording more successes. The number of cases of this crime might be on the decrease while the actual crime level is on the increase. This could be as the results of the gun smugglers or dealers increasing their trade but applying clever tactics and evading the police.

Since a reported case of crime detected as the result of police action indicates a successful arrest by the police, the number of the cases is directly proportional to the number of police successes in dealing with this crime. The increases in all subcategories, based on the SAPS stats such as the 2.4% of illegal possession of firearms and ammunition, 13.6% of drug related crime and 10.6% of driving under the influence of alcohol or drugs indicates the increase in the successes of the SAPS crime combating operations.

1.2.2 Identification of perpetrators through access at SAPS

The police have developed a database management system called the Automated Fingerprint Identification System (AFIS) which is the ICT innovation that has replaced their traditional manual fingerprint processing through automation. Since most of the perpetrators of crimes have to travel to crime spots, the AFIS system being utilized by the police at random and at intelligent driven cordon and

search operations has proved to be effective in reducing the movements of these criminals who they apprehend at random at these operations.

This is because this system is successful in positively identifying the perpetrators or suspects who have been convicted before, or those whose fingerprints were lifted from crime scenes as well as or the fingerprints for suspects who have outstanding summonses. The AFIS achieves the instant positive identification when the suspects' fingerprints are scanned into the system. The AFIS has a database that stores details of all convicted criminals while offering automated addition of new records and random retrieval of any record stored. This system empowers the police to perform quicker and authentic identification of suspects through their fingerprints.

The system is capable of a local and remote connection to other systems where its data collection tool, the MorphoTouch system, has both local and remote connection facility with AFIS database which is stored at police Central Criminal Record Center (CCRC) in Pretoria. This system enables SAPS officials to act promptly after verifying or authenticating the personal attributes or details of suspects. The system uses the biometric fingerprinting capability where criminals, mostly whose fingerprints have been collected at crime scenes or those with fake documents are linked with their fingerprints, arrested and prosecuted (ITWeb, 2007).

ITWeb (2007) explains that the MorphTouch, which is the fingerprinting tool that is utilized by the police to scans suspects' fingerprints into the system, is capable of storing 50 000 (fifty thousand) fingerprints locally while it is able to remotely connect to the AFIS databases at the CCRC. The AFIS database at CCRC is capable of storing millions of fingerprints belonging to convicted criminals or suspects' including the prints that were lifted from crime scenes.

The police system is also proving to be effective with the identification of suspects who have committed stolen identity crimes and running around with their victims' identity documents. Even though they insert the pictures of their faces in the fake identity documents, the AFIS system retrieves their true identities once the MorphoTouch has scanned their fingerprints.

The police have therefore automated their internal access to information and are achieving instant identification of convicted perpetrators. Despite the implementation of e-governance, the police are still not able to identify all perpetrators. This is due to the limitation of the AFIS database which can only identify perpetrators who have criminal records in the database at CCRC. This creates a need by the police to access information held by DoHA which has the identification records of all citizens.

While access by the police to information held by DoHA is currently enabled through manual process, the process does not help the police to expedite their crime reduction efforts as it is too slow to enable the police to identify, authenticate or verify the identities of perpetrators within the legal detention deadlines before charging them. The police need an automated process for instant results and action. This however raises policy concerns of possible policy conflicts.

1.2.2.1 Manual identification by SAPS

The manual identification or processing of fingerprints is still taking place within SAPS where the police at the criminal record centers, both local and the central one manually compare fingerprints of arrested suspects with those lifted from crime scenes to find a match and effect arrests. Otherwise the fingerprints are transported from all police stations and Local Criminal Record Centers (LCRC) which are mostly located within the premises of the police stations to the CCRC where the identification takes place. If there are no matching details of the suspects, then the CCRC transports the fingerprints to DoHA for identification of the owners. The physical handing over and receipts of the fingerprints, to and from DoHA respectively is a manual process even though both the processing for identification at the CCRC or at DoHA may be automated.

1.2.2.2 Automated identification at SAPS

While the police have automated their internal identification process, this has limitations since they cannot identify perpetrators who have never been convicted.

While automation of access to information at DoHA may seem to be the desired solution, this raises policy conflicts which have to be taken into account.

1.2.3 Identification of citizens through access to information at DoHA

The Department of Home Affairs (DOHA) has developed a system called the Home Affairs National Identification System (HANIS) whose databases, the National Fingerprint Identification Registry Database and the Civil database were created by electronically scanning the manual individual fingerprints of all citizens from paper to a digital media. This was done by transferring the details into the electronic media to form the electronic National Fingerprint Identification Database of all citizens.

The database is dynamic as it is continually updated with new comers each time babies are born or with foreigner's information when entering the country legally at ports of entry, borderline posts and airports. The database is also updated ongoing with information of citizens leaving and entering the country as well as death information where births are confirmed with birth certificates and death certificates are issued for deaths. The Department of Home Affairs is cautious and will not allow remote online access to its database which is in line with the legislation in effect for privacy rights.

Access to both HANIS and Civic databases enable identification of citizens and visitors whose details are retrieved when their identification numbers are typed into the systems. HANIS extends the identification process to be achieved through the scanning of fingerprints. Access by other departments to information held by DoHA has therefore become necessary since the latter is the only custodian of the national databases. This however presents policy concerns which are exasperated by the ICT solutions that tend to offer better and faster access by a department, to information held by another department.

1.2.4 The Constitution

The Constitution of the Republic of South Africa Act No.108 of 1996 (hereinafter referred to as "the Constitution"), states that South Africa is a sovereign

and democratic state that is based on, amongst others, the advancement of human rights.

1.2.4.1 The constitutional right of access to information

The Bill of Rights in the Constitution includes the right of access to information in Section 32 which states that everyone has the right of access to: "(1)(a) any information held by the state:" and "(1)(b): any information that is held by another person and that is required for the exercise or protection of any rights" and "(2) National legislation must be enacted to give effect to this right, and may provide for reasonable measures to alleviate the administrative and financial burden on the state."

1.2.4.2 The constitutional right to privacy

Even though the Constitution calls for the rights of access to information to be given effect, the Constitution also calls for everyone's right to privacy to be protected. According to Section 14 of the Constitution, everyone has the right to privacy. The state is therefore compelled to establish security measures that are to ensure that personal information of citizens in public and private hands is protected against unlawful retrievals or disclosures, storage and distribution.

1.2.4.3 The constitutional right to communication

The Constitution takes factors that affect access to information into account and calls for effective measure to be taken to ensure successful communication to or from everyone is achieved. Section 30 of the Bill of Rights in the Constitution guarantees protection for every one against others and also guarantees the right of every one to communicate or be communicated to in the language of their choices. To ensure that this is possible, Section 6 of the Constitution identifies eleven official languages of South Africa.

1.2.5 Access to information policy process

The access to information policy was kick started at the level of a Bill were the initial drafts were referred to as the Open Democracy Bill. Information or Open democracy policy was initiated by the then Deputy President Thabo who set up a task team that started

drafting the legislation amid various consultation processes (Lor and van As, 2002). This Bill provides for the promotion of access to information held by the state as well calling for security measure to be implemented for the protection of such information against privacy violation.

Various initiatives were taken to promote access to information. These include Freedom of Expression and Freedom of Access to Information process, Transparent information policy formulation process and Government policy initiatives on access to information were undertaken at various stages towards formulating access to information policy.

1.2.5.1 Freedom of Expression and Freedom of Access to Information

Like else where in the world, 1994 was a period that was characterized by the rapid developments in ICT systems that were accelerating and providing many easier and faster alternatives of information management including the process of distributing or access to information from anywhere or any institution and by various media or multimedia platforms.

For South Africa, this also marked the period where the government needed to urgently take a look at the way in which information in its possession was organized and how it was made available to the requesting individual members of the public, civil institutions or to other government organs in order to achieve compliancy with the freedom of expression and freedom of access to government information rights as enshrined in the Constitutional Bill of rights.

1.2.5.2 Transparent information policy formulation process

The new dispensation in South Africa since 1994 was marked by a significant change in the style of government with regards to its decision making processes which were driven by the need for greater transparency and public participation. This was being reflected by the transparent policy formulating process which was being adopted by the government. More efforts were made to encourage the public to participate in policy formulation where citizens were requested to provide inputs at various stages of policy making process.

The first policy making stage is the establishment of the green paper which is the first document containing government plans that has taken public inputs into

account. The second step involves the publication of the government statements of policy or intent in a white paper. These policy statements are also made public in various media and related public document. The policy making process also encourages participation by advertisements which include the web addresses from which the public can view or download information (Lor & van As, 2002).

1.2.5.3 Government policy initiatives on access to information

Access to information policy initiatives, according to Lor *et. al*. were started around 1990 and were mainly aimed at ensuring that government information was not only accessible by the public in general, but that strong mechanisms were put in place to ensure the delivery of this information to all corners of South Africa since this was believed to be a key requirement for socio-economic developments in the country.

The initiatives according to Lor *et. al*. include Reconstruction and Development Program that was regarded as a democratic strategy of transparent and participatory government, the Information Society and Development (ISAD) which is a wide consultative strategy of deploying ICT for better public services, universal access and enhancing socio-economic developments, a Task Group on Government Communications that was set up to implementation a Government to Citizens (G2C) communications through multi-purpose community centers (MPCC).

Other similar initiatives include the National Information Technology Forum that was used to survey the implemented MPCC to establish means of strengthening them to achieve their intended purposes, the National Information Project (NIP) was established to adapt the government information sharing strategies through the utilization of ICT to enhance the internal government information management.

The Government Information Project was established to enhance NIP by enabling DPSA to drive the project to improve internal government communication between departments, other agencies and the three tiers of government and lastly the Non-governmental initiatives was comprised of the civil society and private companies like SABINET, Unwembi Communications, Jutastat, Butter-worths and

others that played various roles in ensuring that various mechanisms and structures were put in place to facilitate the availability of government information through various multimedia platforms. While these initiatives were primarily aimed at government providing information to the public for accountability and better democracy, they laid the foundation for access by a department, to information held by another department.

1.2.6 Access to information legislation

Some of the laws governing access to information held by government include but not limited to the Promotion of Access to Information Amendment Act 54 of 2002 which was enacted into law in response to the constitutional requirement for enabling a legal access to information held by government and private bodies and the Protection of Personal Information Bill published on the 14th of August 2009 etc. The Criminal procedure amendment act, No 42 of 2003 was established to, amongst others, guide the police operations involving suspects.

1.2.6.1 Enforcement of accessibility

The Promotion of Access to Information Amendment Act 54 of 2002 (PAIA) is the legislation that was enacted in response to the requirement of the Constitution to give effect to the constitutional right of access to information. PAIA was also enacted to attain various objectives which include but are not limited to, promoting openness and establishing voluntary and mandatory procedures that give effect to the right of access to information in a speedy, cost effective and effortless manner as reasonably as possible.

Even though the act requires that a request for access to information should not be granted if the requested record is covered by one or more grounds of refusal listed in section 11 and 50, the Act requires that such a record, despite being covered by one or more of these grounds, to be accessed and/or disclosed if the contents of the record would reveal important issues that are more harmful undisclosed than otherwise.

1.2.6.2 Enforcement of privacy through protection of information

According to Section 14 of the Constitution, everyone has the right to privacy. It is for this reason that all rights are subject to the limitation clauses which may inhibit access to information under certain conditions. Even though PAIA gives effect to the constitutional right of access to information by everyone, the right of access to information held by the public hands may be limited to the extent that the limitations are reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom as contemplated in section 36 of the constitution. The Protection of Personal Information Bill published on the 14th of August 2009 amongst others, facilitates for the creation of an independent Information protection regulator who will regulate the requirements and codes of conduct with regards to the processing of personal information.

1.2.6.3 The Criminal procedure Act

The original Criminal procedure act 51 of 1977 has been amended through the Criminal procedure second amendment act number 85 of 1997 to regulate the detention of the arrested persons. According to section 1 subsection 1 (c) (ii) of this amendment act, reasonable steps will be taken to have any person who has been arrested to be charged within 48 working court hours. This point to the fact that time is of the essence in processing information necessary for criminal prosecution.

1.2.7 e-Governance development process

South Africa demonstrated its strong commitment to building an inclusive information society in which ICT is effectively utilized and harnessed to attain universal access to information, to contribute positively to socio-economic development and to enable government to deliver citizen centric services, as expressed by the Presidential National Commission in the Information Society and Development Plan or ISAD Plan (PNC-ISAD, 2006).

The Department of Public Service and Administration (DPSA) was tasked with the ICT implementation strategy for which it responded by formulating the IT policy framework (DPSA, 2001). Even though the policy document calls for e-

governance initiatives to address the application of IT to intra-governmental operations (G2G), some related transactions that involve the possible electronic sharing of personal information between departments are not implemented. Instead, ICT initiatives are being implemented at various tiers, the national, provincial and local governments to improve the services or to increase roll out of ICT services to those who cannot afford.

1.2.7.1 E-Governance initiatives at national government

National government offers websites and portals that aid in reducing the need for citizens to travel to a government office for information. The www.gov.za portal is the electronic communication platform and the official website to represent the South Africa government on the internet. The website has various tabs at the top and on the left hand side that have familiar descriptive names to help the citizens to navigate and receive information about government services, where these services can be found, government information, latest speeches by government officials, latest news and various other information about relevant issues that are meaningful to the South African public in general. These may also include information about links to other information, frequently asked questions *etc*.

The descriptive navigation tabs are an effort by government to, amongst others, create an easy one stop shop access to government information that is well coordinated over the net to reduce the possibility of random uncontrolled access to duplicated information that may send conflicting messages to the public (Lor & van AS, 2002). The official government website also will provide links or information about other departments were such departments are still to create their own websites.

Many e-governance initiatives exist, showing various levels of success or failure. Various departments at national level have developed government-to-citizen (G2C) innovations, where access to personal information is automated. These innovations are mostly in the form of websites which can be accessed directly or through the official national government website. Some of these departments which are showing various levels of successes are e-Natis, a national traffic information

system utilized by the Department of Transport: e-filing of tax returns for the South African Revenue Services (SARS) and the remote automated processing of grant applications by the Department of Social Services.

1.2.7.2 e-Governance initiatives at provincial government

Provincial departments have established ICT projects initiatives that also vary from province to province. The Western Cape Provincial Government has launched the Cape Gateway (www.capegateway.gov.za) and the Khanya Project for driving its e-government initiatives and driving schools project respectively. The Gauteng Online Schools project of the Gauteng Provincial Government also serves as another example of e-government initiative that is launched to bridge the digital divide in the provincial schools.

1.2.7.3 e-Governance initiatives at local government

e-Governance at the local government level includes citizen-to-government (C2G) and business-to-government (B2G) transactions, where municipality rates and charges, TV licenses, electricity bills *etc.* are paid through supermarket and post office counters or over the Internet. The major city malls have mostly launched e-ticketing systems for parking where the gate control booms are automatically lifted to enable one vehicle entry when taking the ticket. These are inserted at their machine in the passages of the malls to calculate the parking amount and accept cash before enabling the booms to open and enable exiting of vehicles from the malls.

1.2.7.4 Automated Access to information in South Africa

From the e-governance perspective, the government addresses the foundation for effective G2G communications by setting the Minimum Information Security Standards (MISS) and Minimum Interoperability Standards (MIOS) for information systems through Amendment of Public Service Regulations of 5 January 2001 (RSA, 2001).

While the MISS specifies security standards due to possible integrations of public operations and services, the MIOS specifies the government's technical principles and standards to enable interoperability within and across tiers of

government, as well as between departments (RSA, 2001). These principles and standards as per Chapter 5 of the amendment of Public Service Regulations (RSA, 2001) defines requirements and conditions that are prerequisite for connected and web-enabled government.

1.2.8 e-Governance policy in South Africa

One of the first initiatives for e-governance policy formulation was provided by the country's vision 2014 strategy in which South Africa is described as an inclusive information society where the government has modernized the ICT infrastructure to provide, amongst others, quality services to the communities. The e-governance policy initiatives is centrally coordinated by the Department of Public Service and Administration (DPSA) that consulted broadly throughout government stakeholders (GITO Council) and involved both non-government organizations and civil society in general to launch a national IT policy framework (DPSA, 2001). This framework created the basis for the implementation of e-governance for the public institutions.

The e-governance policy framework also called for the establishment of a central government ICT procurement agency to coordinate the national e-governance development. To achieve the planned government wide e-governance infrastructure and application standardization and modernization, DPSA established statutory coordinating agency, the State Information Technology Agency (SITA) which is to oversee all government ICT procurements to ensure that e-governance was being developed and implemented by all government departments in accordance with the required procedures and standards.

The DPSA policy framework contains recommendations that the policy makers should ensure that the e-government initiative should, amongst others, address the intra-governmental operations (G2G). The Framework also emphasizes that the implementation of ICT was to be done in phases. Since then, there have been various e-governance policy measures and efforts at various tiers of government that

are aimed at utilizing ICT to improve operations which would facilitate better access and services to the communities.

1.2.8.1 e-Governance accessibility policy

The vision of an information society calls for the formulation of, amongst others an enabling policy and regulation that would be used to manage the implementation of an e-government (Farelo & Morris, 2006). The DPSA policy framework contains recommendations that the policy makers should ensure that the e-government initiative should address the intra-governmental operations (G2G), e-services meaning the upgrading of the service delivery models to citizens (G2C) and those of operations that relate to business sector (G2B).

Even though it is generally accepted that South Africa is a front runner with regards to the development of e-government in Africa, the policy makers are still trying to understand various ways in which to proceed with its implementation. The policy makers are for example not certain about the rate at which the implementation thereof should be maintained as well as being able to determine the direction the e-government implementation should take (Maumbe, Owei and Alexander, 2008).

There is a tradeoff situation facing the e-government policy makers of developing countries including South Africa in the form of the existence of two or more types of economies in some of them. In South Africa this is due to the simultaneous dual existence of the capitalist very rich and the impoverished very poor communities who are mostly living without income. E-government infrastructure is basically a very expensive investment which may not likely benefit the poor people who will not only know how to utilize it, but will also not be able to access the services (Maumbe, Owei and Alexander, 2008).

Despite all the effort being put to create an all inclusive information society where the ICT sector is modernized to be thriving and vibrant (Farelo *et. al.*), according to Maumbe *et. al*. the government policy makers are facing this dilemma of alienating the majority of the people who still remain without access.

1.2.8.2 e-Governance Security/Privacy policy

While the implementation of e-government to automate and expedite mainly access by citizens to government information is the preferred and current trends followed by governments, the very nature of ICT processing is making information readily available for many people, local and remote to share. This introduces new security risks of possible unlawful access to information that posse potential threats to institutions and possible violation of privacies of citizens where personal information held by government is involved.

The DPSA policy framework calls for the South African policy makers to employ security measures that are much broader than just authentication and encryption. These measures must include security clusters that caters for thirty minimum requirements such as how to: avoid, deter, prevent, detect, correct and recover from a security breach or damage against, physical, people, infrastructure, applications and information. According to the policy framework, the security policy must provide sufficient details of how these potential threats are to be managed.

1.3 Problem Statement

South Africa ranks high amongst countries that are riddled with crime. The situation is worsened by the insurgent of illegal immigrants who are not registered and are mostly committing crime knowing that the trail of their fingerprints they leave behind will not help the police to identify and trace them. Some perpetrators commit 'stolen identity' crimes by using other people's identity documents as theirs. Others easily pass through the police intelligence cordon and search operations since the police cannot use their personal fingerprint identification system to instantly verify the authenticity of the documents being presented or the criminal record of the person.

The South African Police Services (SAPS) have introduced an e-governance innovation to improve and optimize the crime reduction operations. The utilization of the Automated Fingerprint Identification System (AFIS) has improved the police crime fighting operations. The success of this system is enabled by its database being

able to connect locally and remotely to the fingerprint scanning system, the MorphoTouch. The MorphoTouch is capable of locally storing fingerprints for instant remote identification while it is also able to connect remotely to the AFIS database that is hosted at police headquarters.

Despite the implementation of e-governance, the police are still not achieving the desired crime reduction operations optimization, because the AFIS database details are limited to the criminal records of current and previously convicted perpetrators of crime. The police are therefore unable to identify all suspects. This raises challenges for the crime reduction operations since the police can only detain suspects up to 48 working court hours without charging them. Where they have detained suspects on suspicion of wrong doing, or where suspects are stopped and produce dubious identification documents, the police require instant identification of persons not listed in the AFIS database.

The Department of Home Affairs (DoHA) is the only institution in South Africa that is in possession of the national fingerprint identification database. The Home Affairs National Information System (HANIS) stores personal identification details of all South Africans and legal immigrants. Just like the AFIS, this system has the capability to instantly retrieve the personal identification details of individuals when scanning their fingerprints. The system enables the DoHA authorities to instantly identify any individual in South Africa unless this is an illegal immigrant or in an exceptional case where a person has never been registered.

While access by SAPS, to personal fingerprint identification information held by DoHA does take place, this does not contribute towards enabling SAPS to attain higher levels of performance in their operations. This is because the process is characterized by manual processes with long turn-around times. Currently the turn-around times of the identification transactions of the police at DoHA mostly exceed the 48 working court hours limit set out in the criminal procedure legislation. Since the feedback from DoHA takes longer than the detention limit, the police have to release suspects to comply with the law. This challenge undermines the services of

SAPS towards providing a safer environment for citizens to live in, as wanted suspects may be released due to this technicality.

Even though the information policy enables access by SAPS to personal information held by DoHA, and both departments have implemented e-governance applications to automate their processes of access to information, e-governance is not implemented to automate access by SAPS to information held by DoHA which is necessary to optimize the crime operations.

1.4 The purpose of the research

The background review suggests that policy or lack of it may be inhibiting e-governance with respect to access, by a department to information held by another department where access, by SAPS to information held by DoHA could yield positive results for crime operations. However, we do not have evidence for this. Hence, policy makers and senior public servants are unable to make appropriate revisions to existing policy and practice. Therefore, the purpose of this study is to investigate how policy or lack therefore inhibits e-governance and what policy approaches might enhance e-governance which is necessary for enhancing crime operations.

This will enable the researcher to analyze data from crime operations, DoHA environment, policy environment, including policy, legislation and practice as well as e-governance, in order to understand why automated access, by SAPS to information held by DoHA is not implemented despite the fact that this could enhance crime operations needed for effective and efficient SAPS services.

This analysis will further enable the researcher to contemplate how policy can be used to address requirements for accessibility, security and privacy should these be the issues of concern when proposing recommendations of possible introduction of e-governance to automate access, by a department to information held by another department. The research will therefore analyze the policy environment in terms of:

1) Identifying the relevance of accessibility, privacy and security issues to crime operations and what the privacy and security concerns are.
2) Identifying the extent to which accessibility to information (manual access, automated access) held in DoHA is a barrier or enabler to effective crime operations.
3) Investigating ways in which the policy requirement for privacy of information (manual access, automated access) held by DoHA is a barrier or an enabler to effective crime operations.
4) Identifying ways in which the policy requirement for security (manual access, automated access) presents either a barrier or an enabler to effective crime operations.
5) Identifying how access to information policy and the e-governance policy address the issues of accessibility, privacy and security of information and how automated information sharing can be effectively regulated.

This research will, on the basis of the analysis of the findings, propose recommendations of possible policy amendment or formulation to contribute to effective crime operations within SAPS.

1.5 Research Questions

The following main research question is posed:

How does policy on access to information inhibit or enhance crime reduction operations?

The following research sub-questions are posed:

1. To what extent is accessibility to information (manual access versus automated access) held in DoHA a barrier to or an enabler to effective crime operations?
2. In which ways is the requirement for privacy and security (manual access versus automated access), similarly a barrier or an enabler?
3. How do the access to information policy and the e-governance policy address the issues of accessibility, privacy and security of information?
4. What is the relevance of these policy issues to crime operations?

5. How can policy be improved for automated access to information for more effective crime reduction?

1.6 Chapter Conclusions and Overview of Next Chapter

Detailed descriptions of access to information policy that governs, amongst others, access by a department to information held by another department and the crime situation in the country that points to high levels of crime have been provided. It has also emerged that e-governance can be implemented and utilized to automate access by a department, to information held by another department. Despite SAPS and DoHA having implemented e-governance, this is not optimized for crime reduction. Hence, access to information policy will be investigated and analyzed through a series of questions to determine how this policy is an enabler or a barrier to automated access by a department to information held by another department.

The investigation of access to information policy requires a broad view of the subject matter of the policy environment relating to the relationships between management of crime reduction, e-governance and automated access to information. The literature review which follows in Chapter Two will review scholars' views on key concepts.

CHAPTER 2: LITERATURE REVIEW: REVIEW OF CONCEPTS APPLICABLE TO CRIME REDUCTION AND E-GOVERNANCE POLICY AND PRACTICE

This chapter covers the literature review which is about the reading of articles, books and related other sources of information to enable the researcher to gain the perspectives of a range of authors on how e-governance policy and practice relates to opportunities for crime reduction, through access to information. The review is also informed by reading of and consultations of materials of related concepts such as factors that affect access to information, access to information in public institutions and the right of access thereof. The discussions of these concepts should shed light on the role of information policy in e-governance and how the latter affects crime reduction.

The study operates from the assumption that government access to personal information held by public bodies is necessary under circumstances where this information is required by the police to, amongst others reduce crime. Automated access to information can enable the police to rapidly identify perpetrators, preventing them to commit more crime or bringing them to book. The discussions will also include ways of identifying possible need to either amend existing policy or formulate an effective e-governance policy to enable automated access by SAPS, to information held by DoHA for the identification of perpetrators in order to reduce crime.

2.1 The nature of crime operations

Crime is an illegal action which has been in existence since man came into being and it has been evolving with time (Adeola, Alese and Falaki, 2007). The criminal actions, as Adeola *et. al.* further points out, are generally committed at areas that are normally hidden from view and are usually not easily detected as the areas are mostly from least expected places. Various nations adopt different approaches to crime prevention and combating based on the nature of crime patterns that are specific to them.

Crime reduction operations and planning are now increasing reliance on e-governance to produce crime intelligence through the gathering, analysis and effective communication of information. Because of the diversity of technologies and information management systems, the planning of crime reduction operations involves other units like the crime intelligence that provides the crime prevention and combating operations unit with timely, topical and accurate intelligence policy-relevant information that informs, forecasts and advises on dangers, opportunities and critical developments in crime patterns (Ratcliffe, 2007).

Law enforcement decision makers and executive management are beginning to turn the wealth of information produced through the utilization of e-governance into advantages (Schiller, 2011). This advantage comes in the form of variety of multiple integrated software applications and database management systems which Schiller further explains as the automation of information management that presents information in variety of formats.

The automation presents challenges to the police of processing and integrating the Meta data produced through e-governance with crime information to produce knowledge in the form of crime reduction plans. Ratcliffe (2007) says that the authorities need this process to enhance their decision making to improve crime combating and prevention strategies. Schiller also agrees that the power of crime reduction operations is enabled by the standardization across operational units and the utilization of integrated information.

The crime prevention and combating units would therefore benefit from integrating their plans with units like crime intelligence division which Ratcliffe says it enhances decision making process based on the deeper understanding of criminality in general. This, he says is a strategic thinking that has to do with the type of decision making that can result in a plan that contributes towards crime intelligence in general instead of being a plan for an individual arrest.

Various advantages can be derived by the crime prevention and combating unit for an integrated information management approach by cooperating with crime

intelligence units and other relevant management systems from internal or external sources. Crime intelligence systems offer intelligence tools that support systems integration approaches and are capable of powerful information analysis that produces intelligence needed for all levels of crime management planning.

2.1.1 Crime reduction tools

Most of the crime intelligence officials in general have evolved with and taken advantages of utilizing e-governance. Schiller (2011) says that the police departments that used manual operations to process crime information face numerous challenges such as filing and struggling to find the right information when needed and can not derive synergy benefits of sharing information under such manual conditions.

Schiller further explains that the This system enabled searchable database of crime and incident information which Schiller explains that it enhanced their crime analyzing processes and easier criminal identification through access to information from the databases. Schiller further explains that now officers can quickly access information or share it across different operational areas even when driving in patrol cars.

2.1.2 Integrative design of crime intelligence systems

Crime reduction operations can also take advantage of how crime intelligence systems are designed. This is because the design of crime intelligence system is integrative and inclusive in its very nature. This was evidenced by the Nigerian authorities when they designed their crime intelligence systems. According to Adeola, Alese and Falaki (2007), the Nigerians included various different government agencies and stakeholders' whose information requirements were taken into account to facilitate ease of access to its information by all who are concerned and authorized while it also enables inputs from various internal and external sources. They gathered information from all organizations that were involved in crime related activities and various experts for issues such as crime administration

during the design of their crime intelligence system (Adeola, Alese and Falaki, 2007).

The crime intelligence system is designed to enable for the storage and retrieval of information about crime such as personal identification information of criminals, crime statistics or patterns where various nations adopt different approaches based on the nature of crime patterns that are specific to them (Adeola, Alese and Falaki, 2007). Some designs produced multi-distributed database management systems that could be accessed simultaneously by many individuals or institutions in various platforms while it could also gathers information in the same way.

2.1.3 Intelligence analysis

Data and information collected for the aim of producing intelligence is merely evidence if not processed further or analyzed. Such information according to Ratcliffe (2007) only become crime intelligence once it is analyzed and structured or sometimes when it is combined with other information that may always be readily available or of public nature to produce new information content that contain more meaningful value to enhance strategic decision making. This view is supported by de Lint, O'Connor and Cotter (2007) who refers to intelligence not only as a special case of information and knowledge, but also as an analytically refined product which serves as a package that enhances business operational strategies in pursuit of targets.

Criminal intelligence analysis is designed to support various levels of institutions. According to the Interpol (2011) the analyzed reports can be used to support crime reduction planning at strategic or tactical levels within organizations like the police departments. The system can be used to analyze information and produce intelligence that can provide the strategic level management of the police with early warning signs about potential threats against the country for instance, or to identify potential criminal activity before it happens (de Lint, O'Connor and Cotter, 2007)).

de Lint *et. al*. further point out that the system can also support the operational or tactical management level which may require the system to interact with external sources of information to enable for immediate actions of law enforcement. This could be the authentication of identities of suspects needed to effect instant arrests while the required personal identification information is held by other institutions for instance.

2.2 Access to information policy

According to Jaeger (2007) information policies are implemented to control the process of access to information held by government and are shaping the way government information is made available to the public. This, as Jaeger further explains, is the reason why information policies are regarded as the most influential forces that determine the status of the information society of a country. The policies provide the control measures which are necessary to put in place some limits or security to exclude access to certain types of information where privacy concerns may be sited as the reason for instance.

Access to information policy makers must take various issues that related to access to information into account. These are: factors that affect access to information and the right of access to information in public hands.

Even though ICT innovations can simplify the process of access by a department to information held by another department, it is still necessary to take factors that may affect access to information into account when planning the internal or remote communication channels within or between departments respectively. Buckland, (1991) says that there are six factors that enable access to information which can be categorized as identification, availability, price to the user, cost to the provider, cognitive access and acceptability. The author further points out that even if the source pertinent to the enquiry is made available, successful access to information may not necessarily be gained if one or more of these aspects are not taken into account during communication or planning thereof. Table 2.1 above contains the factors that enable access to information against their brief descriptions.

Table 2 1: Factors that enable access to information

Factor name	Description
Identification	The enquirer may not be able to locate the specific information required even if information is provided to the enquirer. The specific source location has to be identified.
Availability	The physical source has to be available.
Price to the user	The charge in a fee based information service may act as a barrier
Cost to the provider	The providers of sources also incur various types of expenditures like in cases where in archive and library service being offered for free to the enquirer whilst the service may cost efforts, money, space *etc*.
Cognitive Access	Education, level of expertise or unfamiliar language *etc.* may prevent successful access due to some difficulties emerging in trying to understand the provided source.
Acceptability	**(**Wilson as cited in Buckland, 1991) says that acceptability may act as a barrier to access to information for instance, if the enquirer views the source with suspicion questioning its authenticity as lacking in cognitive authority. The enquirer may also refuse to accept the evidence of the source as it is unwelcome in what it signifies and thereby being in conflict with the enquirer's other beliefs. (L. Festinger, A.G. Greewald & D. L. Ronis as cited in Buckland, 1991) names this refusal as a cognitive dissonance.

Source: Buckland, 1991.

2.2.2 The right of access to information in public institutions

The Rights of access to information include rights to create and communicate information in the form of freedom of expression and association, the right to control others' access to information such as privacy and intellectual property, the right to access information in the form of the freedom of thought and the right to read (Mathiesen, 2008). The right of access to information held by government is an international law recognized by many nations. Saxena (2004, p.7) adds that "…the right to information is guaranteed in the international law, as part of the freedom of expression in Article 19 of the International Covenant on Civil and Political Rights".

The importance of the right of access to public information has been investigated by various researchers who all argue that it is a fundamental human right. Mathiesen (2008); Roberts (2003); Saxena (2004) and Sharma and Gopal (2006) refer to the right of access to public information as the touch stone of all forms of freedoms that hold governments accountable while promoting transparency and fairness based on equality for all citizens. This view has long been advocated by

various global institutions including the United Nations General Assembly which adopted Resolution 59(1) to that effect.

2.2.3 Policy requirements for accessibility

Accessibility has long being recognized by almost all democracies including international bodies like the European Union (1995), which put emphasis on this phenomenon through article 1 issued as a directive that prevents restrictions on personal information from flowing freely amongst its member states. Accessibility is widely associated with openness of information in government, partly through the utilization of ICT on functions and services to citizens (G2C).

The integration of the departmental systems to enable information sharing or access by a department to information held by another department is sometimes confronted with various challenges. Some of these challenges may be associated with existing institutional arrangements, organizational structure or managerial bureaucracies which may inhibit the process within government and impede on the possible attainment of government-wide integrated services at a single point (Luna-Reyes, Gil-Garcia & Cruz, 2007).

These challenges could be brought about by, amongst others, the reluctance by departmental heads to integrate or share systems and data with other departments possibly due to the fear of possible harmful nature of leakages of sensitive data or could be due to the lack of some central coordination from executive management (Fan and Zhang, 2007). Fan *et. al*. also argue that for successful accessibility policy formulation to be enhanced, officials from participating departments have to collaborate, negotiate and agree on the protocols that govern the inter-departmental interactions.

2.2.4 Policy requirements for security

During the development of security policy, while great care has to be taken into account with regards to the privacy concerns of citizens for confidentiality of personal information and complying with best and reliable practices (Singh, 2010), the developers must also ensure that production will not be stifled due to restrictive

security policy that may result in production information being protected even against access by legitimate workers who need to process the information in their daily operations (Joia, 2004).

2.2.5 Policy requirements for privacy

The importance of privacy has long been recognized and emphasized by many international institutions like Universal Declarations of Human Rights of 1948 through article 12 and the Council of Europe through its Convention for the Protection of Human Rights and the Fundamental Freedoms of 1950 through article 8. the OECD (1980), the Council of Europe again, through its Convention for the Protection of Individuals with regard to the Automatic processing of personal data of 1981 and other global institutions.

These institutions have come up with rules to ensure that privacy of individuals is not compromised. Some of such rules, for instance, state that personal information must be collected fairly and legally and must only be utilized for the specific intention for which they were collected. According to Henderson and Snyder (1999) privacy is defined as the right of individuals to be in control of how their personal information is collected and used.

2.3 Legislation

Most of the information held by governments is of personal nature containing details of citizens. According to (Sharma & Gopal, 2006), personal information in the hands of government is collected and used specifically for lawful functions and can be disclosed to third parties without the owner's consent strictly if it is permitted by law, if the disclosure thereof is for reasonably necessary for law enforcement or if it is reasonably believed that such disclosure is necessary to prevent or minimize the impact of an impending threat to health and/or life for instance.

2.3.1 Legal access to personal information

In order for the legislation that promotes the right of access to information in the hands of government to comply with the lawful usage of personal information, such laws must provide for details of security measures that need to be implemented

to address privacy issues (Sharma & Gopal, 2006). Personal information may only be disclosed to third parties under exceptional circumstances guided by the provisions of the law. These provisions, according to Sharma *et al.* requires legislation that details and defines procedures for reviews and appeals that may extend to the external independent appeals officer, information commissioner or the ombudsman who must ensure that government acts fairly in deciding to disclose or withhold information.

Sharma et al. further points out that the ombudsman or the courts could be given jurisdiction over such matters depending on the institutional infrastructure of the specific country. This is to avoid the situation that may create room for some of the officials to deny disclosure of information for legitimate requests. Such officials would withhold information that is not covered under any non-disclosure exemption.

2.3.2 Privacy laws versus access to information

Privacy laws are not barriers that impede on access to personal information held by government. Even though article 12 of the United Nations Universal Declarations of Human rights (1948) provides that no individual would be subjected to arbitrary interference in their privacy, and that everyone has the right to the protection against such unlawful attacks, The word "arbitrary" in the declarations below, points towards some acceptance that certain invasions of privacy may be regarded as reasonable based on specific circumstance. Article 29 of the Declarations recognizes limits to the exercise of rights and defines them as those that are determined by law solely for the purposes of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society.

2.3.3 Security laws against rights of access to information

While the laws on access to information in government hands can create the perception that access to information held by governments is unrestricted, no government recognizes any rights of access to information without a qualification and a scope (Roberts, 2003). Roberts goes on to say that in passing laws of access to

information in government, governments define institutions to be subjected to these laws, the circumstances under which these institutions can withhold information and works out the cost and price of the administration required to process the access to information activities.

2.4 The evolution of e-Governance and policy

e-Governance is the second and current step of the evolutionary path followed by the integration of ICT into the public sector which started from the initial e-government step. This is because e-government is described as the initial developmental stage of e-governance (Paskaleva-Shapira, 2006).

While there are various and different developmental stages taken by the integration of e-governance into the public sector which are provided by different authors, Batista (2003) presents three stages which the writer refers to as the stages of the integration of ICT into the public sector.

Batista's stages of the integration of ICT into the public sector are more suited for the purposes of this paper since the stages enable for the drawing of a line that separates and help to differentiate between the concepts of e-government and e-governance whose boundaries seem to overlap in their description by various writers. The stages are tabulated in Table 2.2 above which shows the stage numbers against their descriptions.

Table 2.2 : Three steps of ICT integration into the public sector

Stage No.	Description
Stage one	Technology is only utilized by management in their offices.
Stage two	State provides government non-interactive and unilaterally designed electronic or digital media services to the public.
Stage three	State uses ICT for good governance

Source: Batista, 2003.

Stage one and two undoubtedly points to e-government stage of the development of e-governance since e-government is the initial introductory stage of

ICT where the management of the public service first had to understand it before extending it to various levels within the sector and as services to the public in general. In other words, this is the stage that serves as the initial stage of utilizing ICT to automate government operations or functions as well as the automation of services to the citizens.

The third step describes the e-governance stage and shows that the main developmental stages of e-governance can be divided into two. The first stage is referred to as e-government stage while the second can be e-governance stage. The lines separating the boundaries of these concepts might differ from country to country due to different e-governance policies which are used by governments to control and plan the implementation of e-governance.

2.4.1 e-Government stage

The concept of e-government is not new according to Gordon (2002) since governments were the first users of computers even though the name "e-government" was not used. The emergence of internet has been one of the major drivers of the take up of e-government in the public sector which Gordon also says that the drive to reform public sector also contributed to e-governance take up.

Various international institutions have joined in the wide descriptions of e-government for example (OECD, 2003 and World Bank, no date). The latter defines e-government as government using technologies like the WAN, the internet, *etc.* that are capable to transforming relations with, amongst others, other arms of government for better delivery of government services and improved interactions through access to information.

2.4.2 e-Governance stage

e-Governance has been brought about by the identified defects and cracks that were exposing some limitations of e-government. This is due to the implementation of e-government being due to unilateral decisions by government to automate services to citizens that include other government departments. Despite some advantages and benefits, Paskaleva-Shapira reveals that the utilization of e-

government was mostly faced with constant challenges that threatened to minimize the intended benefits. These challenges faced the public administrators and became too diverse and complicated to be addressed by just the implementation of e-government. Some of them relate to consultation or lack of it that caused the interests of the stakeholders to be excluded from the implementation plans and hence resulting in its rejection (Klischewski, 2011). This, according to Klischewski was because wrong architectures were being unilaterally selected which did not conform to the requirements of the specific contexts.

The process of addressing the new challenges, as Paskaleva-Shapira elaborates, has pointed to a need for the consideration of a new concept such as the adoption of a strategic approach that should be driven by an adaptive policy and regulation and be embraced and used by the executive to control and coordinate co-operations. This has led to the introduction of the concept of e-governance (Paskaleva-Shapira, 2006).

There are various definitions of e-governance that can help to clarify its objectives, for example (see: Batista, 2003; Finger and Pécoud, (2003) and Singh, 2010). Singh defines it as the application of ICT on the functioning of government which accommodates other non ICT concepts that include but are not limited to massive government process re-engineering that also impacts on staff related issues like the disciplinary and motivational activities.

e-Governance can be utilized to address the traditional government departments' limitations of operating separately in silos with little sharing of information to benefit from potential synergies of information sharing. e-Governance' interoperability function has the capability to integrate the systems of local and remote departments while enabling them to be controlled by different individuals who may be locally or remotely located and yet achieving this feet at optimized government operations while lowering the operational costs (Klischewski, 2011). It is through this achievement that e-governance can be utilized to implement

the process of automated access, by a department to information held by another department.

2.4.2.1 e-Governance automation of access to information

e-Governance can be utilized to provide the automation of access, by a department to information held by another department which offers improved and faster ways of sharing information between government departments called government to government communication (G2G). G2G is one of the various communication types that e-governance is capable of enabling. All government departments locally or globally are either in the process of inter-connecting to share information or have already implemented (Klischewski, 2011 and Shapard, 1996).

Shapard further states that governments like the US have been the pace setters that interconnected their departments as early as 1982 when they deployed telecommunications technologies like fiber optic, automated messaging, trunked radio and electronic gateways to interconnect their departments which tended to improve their public administration. Telecommunications benefits were also exploited in the education sector to localize remote rural schools that has a shortage of teachers for instance, by connecting cameras and monitors at both ends to a fiber-optic bandwidth that connected the schools and enabled remote audio and vision (Shapard, 1996). Shapard also say that in this environment, a teacher in the city and the remote students in various village schools could communicate by seeing and hearing one another as if they were all in the same class.

According to Gordon (2002) e-governance can be applied to transform the institutional infrastructure of governments from the traditional hierarchical organizational structures that operated separately in silos of authoritarian top down decision and policy making models to multiple departments or agencies that collaborates through loosely coupled networks. Fang (2002) adds that this can facilitate better communications between departments or tiers of government.

The resulting models enable the civil servants in different departments to collaborate effectively within and across departments (Gordon, 2002). This, e-

governance achieves by its capability to provide the authorities with ICT infrastructure platforms and programs like the internet, which can enable various institutions that are remotely connected to communicate as if they were local.

e-Governance can be utilized to transform the outdated workflows within or between government departments and replace them with established digital links of workflows (Joia, 2004). The integration of services between departments enables governments to offer integrated services at lower costs (Klischewski, 2011; Gordon, 2002 and Khoumbati and Themistocleos, 2006). This is enabled by departments being able to communicate and cooperate better through a single infrastructure that eliminates or minimizes duplication costs (Khoumbati and Themistocleos, 2006).

e-Government can be utilized to achieve two types of departmental integrations referred to as the horizontal and the vertical integrations.

2.4.2.2 Horizontal integration

The horizontal integration refers to the integration of the services of the departments within the same level of government which according to OECD (2003a) enables the departments to achieve cross departmental solutions to complex issues that were traditionally of department specific public policy.

Singh explains that e-governance can be further utilized to ensure that the departments are fully restructured and integrated to exchange and share information to offer the seamless one stop shop services.

2.4.2.3 Vertical Integration

The vertical integration enables the integration of the operations and services of different levels of government departments or tiers of government such as national, provincial and local government to, according to OECD (2003a) "*collaborate closely in order to present a coherent online message to the public*" (p.58). Gordon (2002) argues that a necessary requirement for any government to achieve seamless, multichannel and public-centric packages, the entire government departments or tiers of government must operate as a single organization by adopting

shared platforms for the core technologies on which to execute common applications that have to be consistent across departments.

This, as Gordon puts it, will enable the departments to create solutions that make it easier for citizens, business or other arms of government to access government wide services and information within a single department, or across the entire governmental system regardless of whether it is at national, provincial or local.

2.4.2.4 Automated data sharing model implementation requirements

Work done by Fan and Zhang (2007) indicates that an e-governance communication type government to government (G2G) of automated data sharing model can be successfully implemented to benefit the integrated departments including those from different levels if its developmental requirements, which can be categorized into four, are adhered to. Fan *et al*. also further provide a list of the category requirements and their descriptions which can be found in Table 2.3 above. A number of writers support this information sharing model and are of the view that if the essential requirements for information sharing are met then the departments can integrate their systems successfully (see, Luna-Reyes, Gil-Garcia and Cruz, 2007; Headayetullah and Pradhan, 2009 and Khoumbati and Themistocleos, 2006).

e-Governance technologies like the Enterprise Application Integration (EAI) is capable of integrating different heterogynous technologies from various locally or remotely located departments while offering reliable data transfer, efficient information sharing within and between organizations as well as providing security over the network (Khoumbati and Themistocleos, 2006).

Table 2 3: The requirements of the automated data sharing model.

Implementation level name	Description
Environmental requirements	Refers to, amongst others, the need for the existence of a key requirement for a central coordinating control function or for an officer who has adequate authority over the participating departments to guide the sharing process according to interoperability regulatory framework that defines amongst others, all legal protocols and technical standard which are required to be implemented by participating departments.
Inter-organizational requirements	Refers to, amongst others, the need for the inter-departmental trust that all participating departmental officials will act in the best interest of all participators.
Intra-organizational requirements	Refers to, amongst others, the need for top organizational support to be in place to encourage the process by ensuring that all requirements for effective information sharing are in place and that all participating officials have clear understanding of the logistic movements and handling of shared information. This level also points to a need for effective security measures to protect sensitive information like personal information that might be accessed by unauthorized individuals to violate privacies or be harmful to the participating departments.
Perceived performance requirements	Refers to the perceived benefits and risks as it was found that the perception of benefits can encourage participation while that of risk can yield the opposite effects

Source: Fan and Zhang, 2007.

2.4.2.5 e-Governance security

e-Governance provides various means of security measures that can protect information that is being shared between two or more users who are geographically dispersed in different regions or locations. One of such measures is a tool that can control access to such information over the network and limit it only to its intended users. The encryption technique that renders the information unreadable and useless

to anybody who is not in possession of a decryption key like the Public Key Cryptosystem and Agency Identification for instance, can be applied to decode the information back to readable format (Sharma and Gopal, 2006 and Headayetullah and Pradhan, 2009).

2.4.3 e-Governance policy

e-Governance policy development can be achieved through consultations where the process can be done interactively with other government departments or stakeholders through websites which, according to Michel (2005) and Paskaleva-Shapira (2006) can serve as places for discussions and debate enabling propositions and initiatives to emerge. Michel further points out that policy can be continually be evaluated for instance, by applying key indicators that officials can put in the websites.

It has become important for e-governance policy to include the plans for acquisitions and implementations of the new technologies. Singh points out that during policy formulating stages for the development of e-governance in India, it was found that there were important critical technical issues like how the new technologies were going to interact with the existing infrastructure, for instance, which were necessary to consider in view of accommodating them in the policy requirements.

2.4.3.1 e-Governance policy requirement for Accessibility

The policy makers should plan e-governance policy that would take the new planned ICT infrastructure and its interoperability with the existing hardware platforms and software programs for instance, into consideration to ensure adequate access to stakeholders Klischewski (2011). Since Singh (2010) proposes that e-governance can be developed in four stages, the writer explains that the fourth stage is where the systems and operations of various departments are integrated and able to share databases. It would be crucial for policy to provide guidance on the type of communications of various stakeholders from different departments as well as their levels of access to information for instance.

It is also at this stage of e-governance development where the G2G communications of the departments produce virtual counter services that are enabled by the integrated information from various departments (Singh, 2010). Policy should also include issues of ownership and quality of the integrated information. The quality of information being accessed and shared between various departments for instance can be maintained by the utilization of ICT public key infrastructure to maintain data integrity using MD5 algorithm (Headayetullah and Pradhan, 2009).

2.4.3.2 e-Governance policy requirement for Security

Where two departments are to share sensitive information, the security policy calls for information to be transmitted in secure networks where access to information has to be restricted through the authenticating applications like the requesting of passwords before allowing any access. During the development of policy, great care has to be taken not to stifle production due to restrictive policy (Joia, 2004).

e-Governance security policy should consider various security measures that can be applied to protect confidentiality of information across the network between departments. Headayetullah and Pradhan (2009) suggest that the policy should include secure protocol that protects information for confidentiality that could pave the way for implementing security ICT applications like the Public Key Cryptosystem and Agency Identification using a unique mapping function.

2.4.3.3 e-Governance policy requirement for Privacy

The evolution of ICT led to the creation of rules in relation to automation of processing of personal data by global institutions like the OECD (1980) and the Council of Europe through its Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 1981. Amongst others, some of the rules states that personal information must be collected fairly and legally and must only be utilized for the specific intention for which it was collected.

The security policy developers should take the citizens' concern over the privacies of their lives as well as taking the confidentiality of personal information

into account during designs of public web pages (Singh, 2010). Great care has to be taken by the policy makers for the purposes of ensuring that security and privacy concern are considered for the possible processing of personal data (Klischewski, 2011).

An ideal way of addressing privacy and security issues according to Singh is also by identifying best practices and reliable ways of usage where security measures such as data encryption and Public Key Infrastructure (PK) can be implemented. Klischewski (2011) expresses this view and adds that in order to implement a successful e-government interoperability, the architecture that is based on the reflection of the specific implementation context should be selected to be acceptable by all stakeholders, to standardize all organizational units and be scalable for further integrations and upgrades. Paskaleva-Shapira points to legislative and regulatory barriers or inconsistencies in policy as possible obstacles and challenges that may inhibit the implementation of e-governance if they are not taken into account.

2.5 Conceptual framework

The components of the conceptual framework (Figure 1) include both information and e-governance policies as well as their requirements for accessibility, security and privacy. Other components include e-governance and automated access. Even though SAPS and DoHA comply with the requirements of information policy, which enables access by SAPS, to information held by DoHA, the policy also requires access to information to be lawful and in compliance with the security and privacy policies.

The crime reduction operations of SAPS are not effective and efficient as the process of the identification of perpetrators by SAPS using the identification information held by DoHA is manual and slow. This has resulted in the turn-around times that are longer than the detention period limits that are set out in the Criminal Procedure act and resulting in the police being unable to identify perpetrators in time before the set deadlines. Crime reduction is therefore undermined as the police have to release suspects if they fail to identify them by the set deadline.

SAPS and DoHA are utilizing e-governance to automate access to information for the identification of perpetrators and citizens respectively.

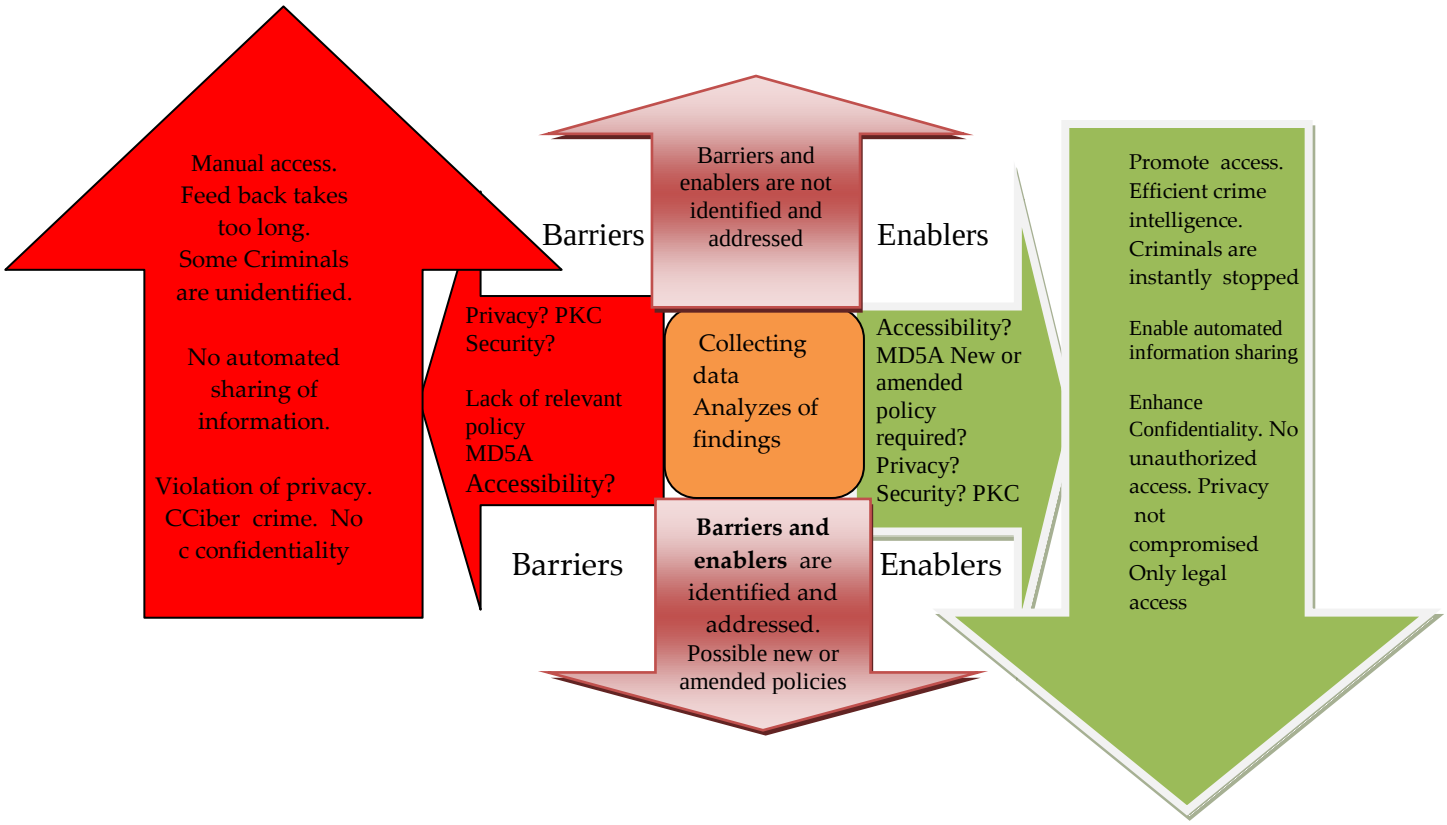
Even though policy enables access, by SAPS to information held by DoHA, and that both departments have implemented e-governance to automate access to information in their possessions, e-governance is not implemented to automate access by SAPS, to information held by DoHA even though this is necessary for the identification of perpetrators to enhance crime reduction. This is despite e-governance complying with policy requirements for accessibility by including information integrity MD5 algorithms and for security and privacy by including technical secure protocols that uses Public Key Cryptosystem (PKC).

The conceptual framework for this research study, discussed above, can be represented as in Figure 2.1 below. The core of this framework and the elements (units of analysis) which are to be studied are:

(a) Possible policy requirements, where issues of accessibility, privacy and security may all be barriers or enablers of e-governance.

(b) Automated access, by SAPS to information held by DoHA, where protocols for data sharing like integrity MD5 algorithms (MD5A) can promote accessibility while technical secure protocols for data encryption can promote security and privacy may all be barriers or enablers of e-governance.

Figure 2 1: Schematic representation of policy impact on crime management



Source: Motlhabane, 2010.

The objective of the study is to examine the relationship between the possibilities of automated access to information versus policy requirements in order to make recommendations for policy on automated access to enhance crime operations.

2.6 Chapter Summary and Overview of Next Chapter

According to the review of the literature, access to information policy is used to control access to information held by a public institution to ensure that information is accessible. This policy also restricts access against un-authorized persons for the purposes of protecting the rights of citizens. In order to automate access to information, access to information policy has to evolve and link to e-governance policy in order that they complement each other, not clash and obstruct

due process. Where a law enforcement department has achieved the electronic integration and automation of access to information with other departments whose information enhances the law enforcement's operations, crime levels are significantly dropped in such environments.

Automation of access by a department to information held by another department can therefore be implemented to optimize the performance of both departments if the planning, development and implementation of e-governance policy and e-governance automation of access are in compliance with development requirements such as consultation and taking the institutional context into consideration.

The next chapter will outline the research methodology to be followed. This provides information on the research design applicable to answering the research questions, how data was obtained and from who, as well as describing the data analysis methods. The research limitation and its strategy are also part of the chapter.

CHAPTER THREE: RESEARCH METHODOLOGY AND DESIGN

3.1 Introduction

Chapter three contains the description of the methodology that was selected for this research to investigate the role of information policy on the effectiveness and efficiency of crime operations. The investigation was done through a case study of the two departments of South African Police Services (SAPS) and the Department of Home Affairs (DoHA). The research focused on how information policy impacts on the implementation of e-governance since it has a direct influence on the development and implementation of e-governance which is needed to enhance crime reduction operations.

The chapter also goes through various areas which are covered and provides the details of the activities that are needed to be carried out from the beginning to the end of the research. These are the research methodology and theory of research, research design, the case study approach, sampling methodology, research data collection instruments, reliability of data for this research, data analysis, significance of the research, limitations of the study, assumptions of the research, research strategy and the chapter summary.

3.2 Methodology and theory of research

This section outlines the methodology and theory of the research for this paper. A qualitative research methodology has been selected for this research. According to Mack, Woodsong, MacQueen, Guest & Namey (2005) the qualitative research methodology is described as a type of scientific research that is consisted of a number of characteristics as follows: it takes an investigative approach in soliciting an answer to a question, it follows a systematical predefined set of procedures to answer the question: it collects evidence: it produces findings that were not determined in advance: it produces findings that are applicable beyond the immediate boundaries of the study: it seeks to understand a given research problem or topic based on the local population being involved while it is also effective in

obtaining culturally specific information about the values, opinions, behaviors, and social contexts of particular populations (Bell, 2005).

Qualitative research has some strengths which researchers take advantage of by utilizing its ability to provide complex textual descriptions of the experiences of the participants over phenomena about which data is being collected to provide information for instance, about intangible human concepts that may often be in the form of contradictory behaviors, beliefs, opinions, emotions, relationships etc (Creswell, 2002; Tellis, 1997 and Yin, 2009). These writers are also in agreement that qualitative research methodology also offers data analysis methods that enable for the investigations and interpretations of large phenomena by breaking it into its smaller manageable components that are easier manipulated and understood.

Qualitative research methodology has the other advantage of offering the researchers the flexibility by enabling them to utilize either of the three commonly known qualitative research methods which are each particularly suited to a specific data collection environment depending on the type of data being collected by the researcher. These methods are according to Mack *et. al.* as follows: Participant observation which is appropriate for collecting data on naturally occurring behaviors in their usual contexts: In-depth interviews which are optimal for collecting data on individuals' personal histories, perspectives, and experiences, particularly when sensitive topics are being explored and: Focus groups which are effective in eliciting data on the cultural norms of a group and in generating broad overviews of issues of concern to the cultural groups or subgroups represented.

3.3 Research design

This researcher has utilized the qualitative research method to explore the role played by policy on crime operations by determining the impact of policy on the development of e-governance whose successful implementation can contribute positively to the operations of crime operations. A qualitative research method is selected for this research because of its advantages over other methods. One such advantage is that the researcher can select its interview data collection method to

gather information that includes abstract concepts that relate to human behavior for instance, like emotions, believes, attitudes *etc.* (Bell, 2005). Interviews were structured since, according to Tellis (1997), it is the type where questions are detailed and set in advance. In this way, interviewees were made to focus on relevant information for accurate answers.

The structured interviews were conducted with individual employees at SAPS, and DoHA where the focus was adopted to ensure that not only typical personal experiences were gathered, but to also ensure that their perceptions and believes for instance, were gathered. These attitudes, which were in regards to both manual and automated access by SAPS to information held by DoHA, has become necessary to enhance crime operations. As people remember and relate their personal experiences, they told their stories based on these critical incidents that took places during their interactions. Barth (2011) refers to this type of information gathering as the Critical Incident Technique.

Accordingly Barth says that the Critical Incident Technique has been used in quality and management literature where critical incidents are described as incidents. The interactions were, in this research the incidents during the interactions between the employees of the two departments for instance, where members of the querying department will remember a specific query incident as something strongly positive or negative. (Edvardsson and Roos, cited in Barth, 2011) explain that the critical incident invokes memories of an individual who will report it as a story.

The interview structure was set to follow the descriptive research procedure in order to capture the story of both departments' employee preferences regarding access, by SAPS to information held by DoHA. It was a semi structured interview conducted by the researcher based on four main questions. The responses were written down just under their specific questions in the interview documents. The questions were somehow of repetitive nature to ensure consistency in the responses of the interviewees.

The script was such that these questions were divided into three and are based on the requirements of the access to information policy and their implications on crime operations. This was intended to unlock the memory and obtain attention of the interviewees. The four categories are as follows: (a) questions regarding policy requirements for accessibility of personal information: (b) questions regarding security of personal information: (c) questions regarding the privacy concerns and (d) questions regarding how the requirements relate to e-governance for crime reduction.

The examples of these questions in section 3.4 are: Accessibility, "how does policy on access to information inhibit or enhance crime reduction operations? "To what extent is accessibility to information (manual access versus automated access) held in DoHA a barrier to or an enabler to effective crime operations?": Security and privacy, "In which ways is the requirement for security and privacy (manual access versus automated access), similarly a barrier or an enabler?" e-Governance, "How do the access to information policy and the e-governance policy address the issues of accessibility, security and privacy of information?" Crime reduction, "What is the relevance of these policy issues to crime operations?" and general, "How can policy be improved for automated access to information for more effective crime reduction?".

3.4 Case study approach

Largely a qualitative data collection and data analysis methodology was selected for an in-depth qualitative analysis through describing, understanding and explaining what people tell the researcher, their views and interpretations of particular situations (Tellis, 1997 and Yin, 2009). The qualitative data analysis was supported by some quantitative statistical data on the frequencies of requests of access to personal information between the departments or on their failure or success rates as well as on their turn around times. Even though a case study methodology has been frequently criticized for its lack of generalization which is due to its single case limitations (Tellis, 1997 and Xiao and Smith, 2006) or its usage being

associated with the data collection method where study participants' behavior are observed (Yin, 1994), Tellis argues that it offers holistic picture of experience.

This view is also supported by Babbie (2004) who asserts that the in-depth investigations capabilities of this methodology produces the explanatory insights of the case under study while providing the results that closely represent the environment being studied (Yin, 2009). Babbie further asserts that a case study can however be able to limit the researchers' attention to the essential characteristics and the specifics of the phenomenon for which data is collected.

The researcher has therefore used the case study method because it reviews practices and approaches with respect to the relevant institutions and the conduct of their officials, namely the Department of Home Affairs (DoHA) and the South African Police Services (SAPS). In this case, the application of a case study methodology produced results for the two departments that offered a holistic picture of experience as lessons were representative of the experience of other parts of government.

The case study methodology was also appropriate for this study because it helped to produce the results that enabled the researcher to perform in-depth investigations on the two departments and obtained explanatory insight behind the reasons for certain approaches and procedures, as well as for the officials' behaviors, perceptions, attitude towards technical accessibility automated protocols and security applications as opposed to manual processes of accessibility and security protocols of access to information in their departments. The researcher has also utilized the case study's capability that enabled the researcher to only focus on the essential characteristics of the phenomenon by limiting the researcher's attention on only the two departments being selected for study. The two departments that are selected will serve as the essential characteristics of the entire government while enabling the researcher ease of use.

3.5 Sampling methodology

Two selection techniques for the sampling methodology of this qualitative research were selected and were both applied to identify the sampling group for this research. The purposive sampling technique and the random sampling technique were combined to identify the interviewees from both departments. Four participants from the Department of Home Affairs (DoHA) were selected from the BVR site in Pretoria while two were selected from Head Office in Waltloo. The last two employees selected where senior ex-employees from Head Office. Their selection was informed by the fact that the fingerprint identification process for the police is centralized at one area at DoHA at the BVR building. This has also limited the number of interviewees to only four from the BVR building and only two from National Office since they provided adequate information.

The eleven police officers that were selected for the study are stationed at six different police stations, a Local criminal record center (LCRC) and a Central criminal record center (CCRC). The eleven officers were deemed enough to provide adequate information since they come from various levels and different police stations from different environments. The six police stations are each located as follows: Garankuwa, Soshanguve, Silverton, Centurion while two are in Mabopane. The CCRC and the LCRC are located in Pretoria and Garankuwa respectively.

All participating police officials and the DoHA employees are provided with pseudo names that were used for the purposes of protecting their identities and upholding the confidentiality agreement which they have entered into with the researcher for the purposes of this research.

The researcher did not follow any standard or procedure when creating the nicknames except to create them in a way that made it easy for the researcher to identify and link them with the right participant. The police officers were selected from different police stations because the finger print process takes place at all police stations. These names and those of the police stations and DoHA office are tabulated in table 3.1 above.

3.5.1 The SAPS employees sample

The purposive selection technique was used to identify the members of the police that could be knowledgeable and familiar with the fingerprint processing. The police officials were selected from the local criminal record center which is located in the Garankuwa police station, CCRC and from the various police stations that were randomly selected through a random selection technique since the police officers from different police stations do perform same services. Where a group of officials qualified to be selected, they were randomly selected. Other police officials were also selected based on the purposive selection technique method from the central criminal record center which is the only gateway of fingerprints that are sent to DoHA for identification purposes.

Table 3.1 : The names and numbers of participants per departments

Area	Dept.	Section	Unit	Participants	Name of participant
Mabopane	SAPS	Terminus	Crime prevention	1	MabCP01
		Loate		1	GarCP02
Garankuwa	SAPS	Zone 5	Crime prevention	1	GarCP01
				1	LCRCT01
			LCRC	1	LCRCWO01
				1	LCRCWO02
Soshanguve	SAPS	Section H	Crime prevention	1	LCRCT02
Pretoria	SAPS	Silverton	Crime prevention	1	SilvCP01
		Hatfield	CCRC	1	CCRC01
				1	CCRC02
		Centurion	Intelligence	1	Intell01
	DoHA	Executive	Management	2	DHAEX01
					DHAEX02
		Operations	Fingerprints	3	DHADR01
					DHADR02
					DHAfin01
		Supplier	Consultant	1	DHACO01
TOTAL				17	

Source: Motlhabane, 2011.

3.5.2 The DoHA employee sample

A purposive selection technique method has been used to identify employees from DoHA who could help to shed light on the processing of fingerprints. These are employees at various levels of the department such as executive and senior management, director(s), assistant directors and employees that are directly involved in the processing of the fingerprints. The senior or executive management that was interviewed comprised only of ex-employees that could be found to be interviewed.

3.6 Research data collection Instruments

Even though the qualitative researchers may use various approaches of data collection method for a specific study (Mills, 2003), this researcher has selected the in-depth interviews as the main source of data that was collected and was only supplemented by other sources such as websites of both departments as this helped to increase the reliability of the research results (Yin, 2003). The interview approach was chosen because interviews provide information that is reliable as it is obtained from individuals with personal experience.

The interview data collection method was also found to be the most suitable for this paper since according to Yin it is an important source of data required for a case study approach. The interview approach was also selected to shed light on the in-depth insights of the departments through the respondents' who understand and will describe and explain the incidents of their personal experiences (Tellis, 1997) which provided the researcher with their views and interpretations of particular situations.

A semi-structured interview schedule was developed for the interviews and conducted with the relevant employees of DoHA and SAPS. This enabled for the gathering of information with regards to their attitudes and perceptions on policy requirements being accessibility, security and privacy of information. Interviews were also selected for this research because of the various other advantages that they present to the qualitative researcher which include but are not limited to enabling the researcher to adapt the interview questions interactively as more light is shed and

insight gained to follow up on new phenomena that the researcher was not aware of prior to setting original questions (Bell, 2005).

This advantage has enabled the researcher to adapt the questionnaires ongoing when the initial ones referred too much to policy which some of the respondents seemed not comfortable about. The adapted questionnaires, which mainly refer to procedures and actions, were more easily understood and responded to by the participants. The researcher could easily link their actions and practices back to each policy requirement. For instance, where the participant explains how safely they file information, this is interpreted as being in compliance with the security requirement of policy without involving the participant with the policy jargon.

3.7 The reliability of data for this research

In order to ensure that the findings of this research were reliable and valid, the researcher has selected an interview approach where interviewees were carefully selected through the purposive selection technique to ensure that the findings were reliable which Silverman (2004) says that it is one of the main conditions for the acceptability of the research findings. The researcher also took other conditions such as the consistency of the findings as raised by Neuman (2003) amongst others, into consideration.

The reliability of the findings in this case is upheld if the measuring technique or instrument is used to perform measurements of allowable variables while all other factors are kept constant can produce the same results when performed more than once (Bush 2007). To ensure this, the interview sample group was comprised of respondents who had the same characteristics in terms of personal work experiences within each department and were asked same questions to which they provided same responses.

The responses were consistent even when same questions were asked differently. The technique enabled the researcher to improve the accuracy of the findings as the informants demonstrated consistency through the repetitive questions

and provided more clarity which helped to minimize potential mistakes or errors as well as addressing individual conflicts. In this way, the findings could be regarded as true reflections of the respondents' experiences and views which in turn are taken to be reflective of the departments which were being investigated. The researcher has therefore demonstrated that the results were valid (Bush 2007) and credible enough to ensure that the research can be relied on (McMillan and Schumacher, 2006).

Great care was taken to allay suspicions as the research targeted two very sensitive departments whose employees have been sworn to secrecy because of the nature of the business they are conducting. The researcher was in possession of the appointment letter that was used for the introduction at the management level of each department upon entry. Appointments were only made through each departmental communications' channels from higher authorities. The appointment letter was in the letterheads of the university and had the researcher's identification details, study area and the purpose of the research. The letter also contained the confidentiality clauses which guaranteed the potential interviewees that their names would not be revealed in the research report.

Even though the questions were in English, efforts were made to explain any uncertainty that emerged and the researcher was quick to accept it if the interviewee did not know the answer. The appointments were made with the interviewees in such a way that the interviewees chose their suitable dates, times and places. To enhance ease of communications and foster better relations with the interviewees which according to McMillan *et. al.* is a necessary requirement for conducting a successful interview, some of the interviewees who engaged in lengthy and irrelevant answers that took long times were not interrupted but were eventually brought in line.

3.8 Data Analysis

A qualitative research data analysis method was selected for this research to identify common themes out of the volumes of data which was divided into categories of these themes without altering or distorting the description of the entire process of access or automated access, by a department to information held by

another department which is needed to optimize crime operations. This is because a qualitative data analysis offers a researcher the advantage of investigating and interpreting a large phenomenon through the study of its smaller components (Creswell, 2002; Tellis, 1997 and Yin, 2009).

The smaller components of this research are based on the research questions where the responses of different participants to similar questions were grouped together as categories of themes that were analyzed separately. Since in this way qualitative data analysis enables the qualitative researchers to describe, understand and explain the response of the participants, (Creswell, 2002; Tellis, 1997 and Yin, 2009) the process provided the researcher with an in-depth explanation of whether the information policy plays a role in possible access, by SAPS to information held by DoHA. These explanations are necessary since the automation of access to information between the two departments can possibly determine the effectiveness and efficiencies of crime operations.

In order to understand the current communication status between the two departments, the researcher divided the role of policy on the implementation of e-governance into smaller components which are the policy requirements for accessibility, security and privacy. Each requirement was further divided into various groups of common themes. As mentioned earlier, these themes are based on responses to same question by different participants. The study therefore analyzed the possible indirect role of policy on crime operations through the analysis of the impact of policy on e-governance since as mentioned earlier, the latter has a direct impact on crime operations through automation of access by a department, to information held by another departments.

The in-depth qualitative data analysis of the impact of the policy requirements on e-governance's automated access, by a department to information held by another department was therefore able to provide insights into the current state of affairs that relate to automated access, by SAPS to information held by DoHA. The findings have located the research data within the conceptual framework of a public

administration where the performance of the administration of SAPS' can be effective to provide better services to the community.

The framework was also used to help separate and maintain the identities of the key concepts within policy and e-governance's possibility of automating access, by SAPS to information held by DoHA. The requirements of policy, which formed the key concepts or the units of analysis in the framework, are accessibility, security, privacy and include all other relevant policy issues that emerged. The findings from both SAPS and DoHA are accordingly categorized into themes based on these units.

3.9 Significance of the Study

The study has contributed towards optimizing the crime operations system to enable SAPS to be effective and efficient in their operations. This is to be achieved by recommendations towards formulation or amendment of policy for e-governance to create, if accepted, an enabling environment that can enhance the implementation of e-governance to automate access, by SAPS to personal information held by DoHA to enhance crime operations needed for optimized SAPS' services.

Since the findings are possibly reflective of the communication between all departments of government, the lessons learnt should provide solution for the entire government to improve the public administration. This study therefore also aimed to contribute to the entire government or public operations and administration to be effective to provide efficient public services to the community.

3.10 Limitations of the Study

The accuracy of the findings of the research is limited to the information provided by the interviewees and this could be based on their perceptions and attitude towards their departments. This may however not be reflective of their current situations since the researcher has no guarantee that the interviewees where completely providing true reflections of the departments and their interactions. The interviewees did not know all the answers per questionnaire documents which caused most documents to contain responds of more than one participant.

3.11 Assumptions of the research

The study is performed under the assumption that vetted and security cleared police officers will not engage in fraudulent and corrupt activities like intentionally breaching the security laws and leak sensitive or personal information to unauthorized individuals or criminals. It is also further assumed that these officials will always tell the truth during interviews.

3.12 Research strategy

The research was commenced at the beginning of November 2010 after the approval of the proposal report in October 2010. The development of the interview instrument and creation of the list of the interviewees took place in December and January 2011. The first three chapters of the report were written in February to April 2011. Data collection was done during May to July 2011. Chapter four and five were completed in December 2011. The entire report was completed in March 2012 and submitted for marking. The corrections were completed and the final report submitted at the end of September 2012.

3.13 Chapter summary and overview of the next chapter

This chapter contains the details and descriptions of the methodology that includes a case study which was used for a qualitative data collection that was selected for this research as well as the reasons for its selection. The steps that were taken to complete this research are also detailed in this chapter and include but not limited to, research design, sampling group, data collection and analysis methods as well as the research limitations and strategy.

This has shed light on how data, which will be gathered and documented in the following chapter four, will be gathered, reported and analyzed. Chapter four therefore will provide the findings which will be analyzed in subsequent chapters.

CHAPTER FOUR: CASE STUDY OF SAPS AND DoHA

4.1 Background to SAPS Environment

The findings presented in this chapter were collected from the organizational case study of the South African Police Services (SAPS) in connection with the role of policy in the police' crime reduction operations. Policy comes into play when the situation arises where it becomes necessary for the police to access information held by the Department of Home Affairs (DoHA). The police require this process to prevent and combat crime by using the personal identification information from DoHA to identify all perpetrators of crimes or suspects. The developments in ICT also offer alternative and better ways of improving ways of access to information through automation.

4.2 SAPS' key policy objectives

The police' performance of crime reduction operations includes the need to identify all perpetrators of crime to take appropriate action of either arresting or releasing them. The identification of all perpetrators can only be achieved if access by SAPS, to information held by DoHA can be enabled. While there is a specific police strategy and policy that guide the operations of the police and describing their mandate, the process raises broader policy concerns that must be taken into account.

4.2.1 Crime reduction objectives and policies

In terms of the Constitution, the objectives and policies of SAPS are to prevent, combat and investigate crime: to maintain public order: to protect and provide the security of the inhabitants of the Republic and their properties: to uphold and enforce the law: to create a safe and secure environment for all people in South Africa: to prevent anything that may threaten the safety or security of any community: to investigate any crimes that threaten the safety or security of any community: to ensure that criminals are brought to justice and: to participate in efforts to address the causes of crime.

In order to achieve these mandates, the police have, amongst other, also implemented an Automated Fingerprint Identification System (AFIS) that has enabled them to automate the identification process of perpetrators of crime.

Various policies, some of which have been enacted into law, are used to guide the police operations. Some of the legislation like South African police service amendment act No. 57 of 2008 provides guidelines for enhancing the capacity of the South African Police Service to prevent, combat and investigate all types of crimes including national priority crimes. This legislation also enables the facilitation, reviewing, monitoring and improving the inter-departmental co-operation. Other legislations like the criminal procedure amendment act, No. 42 of 2003 and its other related amendments amongst others, guides the police with the detention periods of suspects without charging them.

4.2.2 Identification of perpetrators

SAPS, as opposed to DoHA storing all citizens' personal identification information, only store and process personal identification information of convicted criminals. The information is stored in a Criminal record database which enables them to track all criminal records of previously and currently convicted criminals. The police utilize AFIS as the system that runs the criminal record database to attain objectives of identifying all perpetrators of crime through their fingerprints that are stored as retrieval keys of the criminal record database stored at the Central Criminal Record Center (CCRC) in Pretoria. While the identification of perpetrators can be done remotely from the police stations through an identity number, all fingerprints identification take place at the CCRC to which the prints are physically transported for verification and authentication to identify the suspects positively.

The identification process at SAPS through access to information in their possession works very well in enhancing their crime reduction operations as long as the perpetrator whose information is being queried has been convicted and therefore has a criminal record. In this case SAPS has no difficulty in a rapid identification through an identity number or fingerprints. Where the suspect or a perpetrator of

crime has never been convicted before, SAPS has no record of such an individual and can therefore not positively identify, verify or authenticate their true identity through the normal operations of access to personal identification information in the AFIS database.

Where the matching details are retrieved, the police are able to act swiftly in their crime reduction operations. This is in contrast with the situation where the matching prints are not available in the criminal record database. If it is important for crime operations for the suspect to be rapidly and positively identified, then the police have to resort to DoHA for the identification of the suspects.

4.3 Findings of accessibility policy at SAPS

The accessibility requirement of policy in this study is about how access by SAPS, to information held by DoHA should be maximized to optimize the operations of crime reduction. This means that SAPS should adhere to certain procedures to comply with the accessibility requirement of policy. This may, for instance be to provide DoHA with justifiable reasons for requests for access to information. SAPS should create information management procedures that instill confidence at DoHA that information obtained in this manner will be used in accordance with procedures that will be in compliance with policy for crime reduction, including rapid detection and prosecution of criminals.

While the current manual access by SAPS to information held by DoHA has become insufficient for the effective operations of the crime operations at SAPS, the developments in ICT seem to be offering better, faster and accurate alternatives. These innovative alternatives may bring improvement in operations, but are accompanied by challenges that need to be evaluated against the benefits. The police are putting procedures in place to ensure that they maximize the benefits that are offered by ICT while minimizing the possible threats or risks associated with its implementation.

4.3.1 Manual access to information

The participants emphasize their commitment to follow procedures and explain various methods followed when taking fingerprints from individuals and suspects. GarCP01explains that, "when we take the fingerprints of an individual who is making an application for a firearm or for a public driving permit for instance, the prints are only taken for one specific application and we only use them for that purpose". He goes on to say that each application is accompanied by its own set of prints which are never used for any other purpose except to check if the person is qualified for the applications which they are applying for.

Another fingerprint processing example came from LCRCWO02 who is in the Local Criminal Record Center (LCRC) which is located at the Garankuwa police station:

Where we obtained the prints from crime scenes, we try to process them here locally and manually in the dark rooms but we also send copies to the Central Criminal Record Center (CCRC) in Pretoria. We investigate if the owner or the suspect has a criminal record or any outstanding summons. If he or she has any criminal record, we will immediately retrieve their identification details otherwise if our systems do not have the matching prints, then we cannot identify the individual. This is when our branch in Pretoria takes the case up with the Department of Home Affairs (DoHA). Our colleagues at CCRC send the copies of the prints to DoHA to retrieve the personal identification details of the owner.

The SAPS feel that they are justified in seeking access to personal information held by DoHA as this is in line with the policy requirement of right of access to personal information of third parties to protect the right to safety of citizens. In requesting access to personal information from DoHA, which is a public institution, GarCP02 had this to say:

We state clearly in the application forms which we are required to complete for each request, the purpose for which information is needed, our identification details, rank, our stations details and commanding officers, who must also attach their signatures

before the applications are considered. After usage of such information, this must not be stored for other eventualities but the information is destroyed if we have no further use of it. For instance, where fingerprints are successfully used to retrieve personal identification details of suspects at DoHA by the police and the suspects are linked with their fingerprints and become incriminated where after they are charged, the personal details are destroyed if the suspects are acquitted.

Since only authorized and expert officials are allowed to lift fingerprints where their expertise enables them to provide evidence which the courts can find admissible, it is accepted that such officials will respect the law and provide reliable and accurate information. The privacy of citizens is deemed as being protected as such selected officials are expected to comply with the policy requirements of handling the information competently or deleting it if the suspects are cleared by the courts.

4.3.2 Automated access to information

The police believe that compliance to policy cannot be compromised by ICT since they believe that the same compliance as in manual processing is maintained except that the technology will provide faster access. As with manual access, they say that information stored electronically is only about the suspects or individuals being queried and it is used for the stated purposes while it is destroyed if the cases against the suspects are dropped. Scanned fingerprints that the police submit for fingerprints' owners' details at DoHA will only be processed if the SAPS application documents contains all the authentication details mentioned earlier under manual requests.

4.3.3 Manual accessibility policy procedure

Manual fingerprint processes include completion of various documents at local police stations depending on the situation at hand. When an individual approaches the police and requests services like a driver's public service permit, they take fingerprints onto the enquiry SAPS 91 document and fax to the CCRC in Pretoria while the original documents are sent to the LCRC. The SAPS 91 document

is used by the police to enquire from CCRC in Pretoria whether an individual is a criminal or has outstanding summonses.

The police use the SAPS 76 document for the same process if the individual has committed a crime while LCRC also uses it to obtain fingerprints from crime scenes. To distinguish fingerprints of non-suspects from potential suspects' found at the crime scene, like household members, SAPS 192 documents which takes portions of hands and fingerprints, are used and follow the same process as that followed when using the SAPS 91.

The CCRC minimizes chances of querying fingerprints of wrong or innocent individuals who are not supposed to be investigated and whose privacy could be jeopardized by authenticating the requests for fingerprint processing from various police stations and LCRC'S.

According to SilvCP01 who occasionally requests personal identification details of the suspects whose fingerprints are lifted from crime scenes:

The central criminal record center at Pretoria will refuse to accept the prints application forms if they do not contain the mandatory requirements details like the requesting police station, the case number, the investigating officer, the identification and contact details of the commander in charge at the police station and his or her approval signature.

He goes on to say that failure to comply results in, "our investigations taking too long as you are sent back and forth due to the court dates of suspects being postponed while waiting for their personal information details".

4.3.4 Automated accessibility policy procedures

Just as in manual requirements, the police must complete the application forms to be accepted by the officers at the CCRC where after authorized police officers are allowed access to the civil person's database at DoHA where they can try to retrieve the personal identification information if they have identity numbers of suspects. Where the fingerprints were taken in full for both hands' all ten fingers, the online verification system, the Home Affairs National Identification System

(HANIS), the personal identification database which stores fingerprint identification, retrieves the fingerprint owners' details almost instantly and these are given to the authorized police officers from the CCRC.

In cases where the latent fingerprints were randomly taken and the owners' details are being requested by the police from DoHA, the latter provides a duplicate civil database and allows the authorized police officers to have direct access to retrieve identification details. According to the police, this process takes too long since the records in the DoHA have been stored by sets of hands plus all ten fingers. CCRC01 says that:

DoHA officials have told our members that HANIS has stored the fingerprints as pairs of both human hands and their ten fingers to be read simultaneously as one key that identifies an individual. If an attempt is made to read just one finger, then the system returns a blank or in most cases it retrieves details of a wrong individual. This also takes long because the system has to read each ten fingerprints of millions of South Africans to compare and find a matching print. Because of this, DoHA has told us that they do not have enough manpower to sit around during office hours and query the database which also consumes a lot of the system's memory and disk space resources. This results in slow delivery performance of the system and frustrates other daily operations like identity and passports processing.

Since a lot of the computer capacity resources are consumed in this way, LCRC01 says that this has prompted DoHA to create a duplicate civil database which the police can query daily without disturbing DoHA's normal daily operations. This database is in the premises of DoHA. According to the police, only the authorized police personnel have been granted permission to gain entry into DoHA offices to access the system.

This has enabled the police to do a search type one to many, which is a process of scanning one fingerprint against all ten fingerprints of an individual's two hands for all South Africans, as they scan one finger's prints and scan through about 40 million times. This can take up to three days at times to find a match if any. The

police say that the success rate for this process is very low. This is in contrast with a process where the ten fingerprints of an individual are scanned into the live Home Affairs National Identification System (HANIS) database where an instant match retrieves the personal identification details of the fingerprints owner almost immediately.

One police officer says the police could previously key in the ID of an individual into the National Population Registration (NPR) and identify them from the database which contains the individual's name, address, age, date of birth *etc*. which was stopped and privacy reasons cited as being the cause.

4.3.5 Concerns regarding manual access

Manual fingerprint processing is difficult and in many cases not successful as some fingerprints need to be taken onto paper several times before being readable. Long periods up to several weeks elapse before details are provided by DoHA. In terms of the LCRC, where an expert has to physically go through many fingerprints and do a manual comparison, most of the prints are not easily readable due to lack of visible characteristics which results in the process becoming cumbersome and time consuming.

Where the CCRC, which is the only national SAPS' gate way to DoHA, sends fingerprints to DoHA, many of them on many occasions come back unprocessed due to being of poor quality and unreadable. This causes delays in the SAPS crime operations. "The process of automating access to information held by DoHA can never be achieved because where the personal identification details are requested by the courts, then the courts require the documents to be signed by a DoHA Director General", according to SilvCP01.

There are various other challenges with regards to prints submitted to DoHA. These may be complicated by tampering of scenes of crime or unrelated prints lifted from scenes of crime for instance those of relatives or family members'. While manual feedback from DoHA takes time, it sometimes returns unexpected results for

instance where a woman's details are provided while the police are convinced that they have submitted a man's fingerprints.

4.3.6 Concerns regarding automated access

Intell01 describes the costs of ICT as being inhibitive to the implementation of automation of access by SAPS to information at DoHA. In his words, "technology is expensive and cannot at this stage be deployed at all police stations or at intelligence driven cordon and search operations". He further points to lack of skills amongst the officers which can also be a stumbling block.

According to police inspector CCRC01, the police at CCRC used to have automated access to the DoHA system for instant identification of suspects or individuals by typing their identification numbers into the system. The process would retrieve the suspects' names, gender, addresses, but this access has been taken away due to DoHA claims of irregularity of use by the police. Now the same process that used to be done instantly takes up to six weeks or more. Other challenges are that the SAPS officials will not be able to utilize DoHA systems due to lack of training on operating the system.

4.3.7 Relevance of access to identification of criminals

By being able to access the DoHA database the police are able to rapidly identify all or most criminals who are not in their AFIS database and this contributes directly to the performance of crime reduction like the cordon and search operations. The operations would be effective if information at DoHA could be accessed to help identify suspects or owners of fingerprints obtained from crime scenes to reduce the backlog of unresolved cases or to quickly charge arrested individuals to shorten the queues at the courts. Intell01 confirms this need for access by SAPS to information at DoHA as follows:

If the personal fingerprint identification details at DoHA database can be retrieved via the MorphoTouch then our criminal intelligence system can be very responsive at all times. If this can be achieved anytime as when we are in operations and identifying anyone, then we can utilize the system to stop many criminals. This can

prevent many more occasions of crime being committed. The system can enable us to nail the suspects who have not only stolen or robbed their victims' cars, but who have also stolen their identity documents to fake their own identities and impersonate their victims. They drive the victims' cars past intelligence's cordon and search operations as they replace their victims' pictures with theirs in the fake identification documents. Impersonation is one of South Africa's main concerns at the moment due to the high numbers of illegal foreigners who are desperate to stay in this country and the corrupt DoHA officials who try to cash in by selling the fake identity documents to these foreigners as you might have seen even on media reports recently. Randomly retrieved information at DoHA can be integrated with the intelligence for instant answers to the police crime operations strategies and operations. Suspects can be arrested with immediate effect and charged within the 48 hours limit which the cops are required to detain before charging. This can also discourage criminals from impounding cars and driving around while the illegal foreigners will refrain from stealing and faking identification details, moving around or driving around. The police's success with the current convicted criminals' record retrieval through the MorphoTouch can be expanded by DoHA information to help them to bring the national crime under control.

DoHA is the only institution that can provide national personal identification information which can contribute to the productivity of the crime operations programs where local and remote identification of suspects with fake identity documents can be rapidly and accurately identified through fingerprinting in most cases.

A SAPS' officer at Garankuwa LCRC says that court turn around times can be improved due to a faster rate of charging suspects where if they are successfully convicted, they could be removed from society for the safety of all. This, according to the officer, could resolve most of the cases for instance, where criminals steal other individuals' identity documents and for instance, when suspects are arrested even if it is for other crimes. Suspects who do not possess identification documents

can be instantly and accurately identified while other police officials who are processing the applications for fire arms and public driving permits can expedite their daily operations.

4.3.8 Access as inhibiting the identification of criminals

"While we require to access information at DoHA for purposes of combating and prevention of crime, like a gun, if sensitive personal information is made available to some of our members who are corrupt, it can be dangerous as they can pass it to criminals for money", this is the view of Intell01 who also says that the presence of illegal foreigners creates the situation where some of them buy identification documents from corrupt SAPS officials or even from DoHA employees as seen on the media. Intell01 also warns against access to information where there are no control measures because this can:

…cause problems at possible three levels at which access to information procedures must be followed to ensure that information is transferred according to protocols and make sure that it becomes helpful to us. The first step is about how we obtain information during normal operations. This should be lawful otherwise it will not help our cause as evidence in court. Secondly at CCRC where the credibility may be jeopardized through contamination as you might have heard in some cases where sensitive evidence documents can go missing or fingerprints documents becoming damaged where the prints become unreadable and not being able to be processed to identify the owners. At the third level this can be at DoHA self where the same challenges may occur. Accessibility therefore may work against crime operations if it is carelessly enabled without proper controls to ensure validity of results to prosecute the criminals without doubts. Otherwise real criminals may be set free through carelessness and technicalities.

If access is not properly controlled, information about the police planned cordon and search operations for instance can be leaked and be made accessible to the criminals who will adapt and modify their operations to be smatter than the police. This, according to the police could undermine the law enforcement initiatives

as criminals gain access to crime operations and increase crime due to these criminals always knowing in advance what the police are planning for them. In all these instances of access to information, attempts must be made to avoid any unauthorized access which in such cases would work against crime operations.

SilvCP01 explains that:

Access to information can be dangerous and easily inhibit crime operations if the sensitive personal information like the names and addresses of the honest and hard working police officials who are on the tracks of dangerous criminals as well as their plans of operations may be leaked to these dangerous criminals who may be assisted by corrupt police officials who act as their contacts from within. This will not only undermine the crime prevention strategies, but also put the lives of these officers and their families in serious danger.

DHAEX01 is also in full support for access, by SAPS to information held by DoHA and provides and example of disadvantages that may occur if access to information requirement is not complied with when he says that,

Non accessibility means that the only department that can provide personal identification information that is so vital to crime operations is denying access with the results that criminals with multiples fake identification documents can elude the police and compromise crime operations. The insurgence of undocumented immigrants presents the country with the biggest headache currently which creates a platform for various crimes committed by criminals who cannot be traced or identified since crime reports would not be able to help due to the lack of access to DoHA which is capturing the details of legal and most of the illegal immigrants.

If an individual's fingerprints are scanned in the SAPS database and draws a blank, then the police would assume that such an individual has never be convicted or has no outstanding summonses. But if the same action performed on DoHA yields the same results, then the police have to detain such and individual as a possible suspect. Where such individuals are found to be foreign criminals, then some crime may have been prevented by apprehending the suspect where more

crime could be exposed due to the police action. In this case, access to information inhibits crime operations if it is denied. The other reason of possible denial of access, by SAPS to information at DoHA may be as presented by CCRC01:

If the DoHA is not assured that we and other police members from the stations may fail to protect the personal details obtained from DoHA and we further fail to convince them that only authorized access will take place to use the personal information solely for the specific purpose of identification, again, DoHA may deny access by SAPS to personal information in its possession.

If there are no proper control and procedures in place, information may be easily and randomly be accessible even by wrong individuals who might jeopardize police operations by knowing, for instance, personal details of all key stakeholders or potential witnesses in crime operations and court hearings. This might threaten the safety of such stakeholders who might stop, out of fear for their life to cooperate with the police.

4.3.9 Manual access as a barrier to crime reduction

SilvCP01 says that, "Manual access by the police to personal information held by DoHA may act as a barrier because it does not always yield accurate results or the turn around times are too long for effective crime operations which amongst others, require processing of information to provide the verification details fast and within detention deadlines". He also goes on to say that the police have only 48 working court hour's limit to detain suspects before charging or releasing them. Manual access to information from DoHA does not help the police to clear or charge a suspect within this limit which has come to undermine crime combating at times.

The police are in most cases frustrated when the fingerprints are returned unprocessed by DoHA which says that the prints are not clear and readable. If the suspect is on bail, they have to wait for the court date to retake the prints which further takes months before feedback. This effectively becomes a barrier to effective crime operations by amongst others, congesting the courts and slowing the criminal investigation process.

4.3.10 Manual access as an enabler to crime reduction

Where manual access by SAPS to personal information held by DoHA is successfully achieved, this ensures accurate identification of suspects or individuals whose fingerprints are not captured by, or do not exist in the SAPS' AFIS database and therefore enables crime operations to process correct and accurate information for effective crime operations. In this case, criminals are linked with their fingerprints which might have been collected at crime scenes to enable the police to arrest, charge and have suspects prosecuted.

Any piece of information that leads to productive successful action is important regardless of how it is accessed. Personal identification details retrieved manually from DoHA enhances the crime operations by positively identifying suspects and criminals and linking them with their fingerprints and crimes where applicable.

4.3.11 Automated access as a barrier to crime reduction

The police assume that DoHA, like any other institution, has security concerns about the HANIS systems' database and believe that the onus lies in their hands to foster confidence within DoHA personnel about their ability as the police to maintain the safety of the personal identification information from DoHA if automated access can be implemented.

They believe that the DoHA may be having fears of security risks where hackers or fraudsters can also gain access through automation to commit cyber crime by unlawfully gaining remote automated access and contaminating information where illegal foreigners for instance, might obtain fraudulent identification documents and crime operations would be fed wrong information by DoHA. This and other such crimes due to possibility of unauthorized automated access would yield bad results for crime operations. The police officers may also not be up to speed with the current ICT programs. Intell01 feels that:

…lack of skills on the police to operate the systems or to understand the way reports are written by the ICT systems since the enquirer may be the officials from police

stations where ICT is not installed yet may also inhibit the effectiveness of crime operations.

The police officers are as the results of this skills shortage not allowed at DoHA to have direct onsite access to their operating system but perform the transactions for them where only the complete set of the ten fingerprints for both hands are scanned to instantly retrieve the identification details of the print owners. This may inhibit the crime operations since the police have to rely on the DoHA personnel to do the retrieval for them which might not always be at the rate required by the police or the DoHA personnel may not always be available or ready to do the automated process for the police.

Automated access to information process may be fast but hackers may also access the system to harmful results. Even though this process is automated, the security requirements for approval and releasing of information might still be manual and slow inhibiting on effective crime operations. If the requirements also do not allow remote automated access, it means that police cannot always instantly identify suspects for prompt actions. Even though automation can provide rapid results, the police still depend on DoHA employees while they do not have authority to push for co-operation from the DoHA employees. Access rights to DoHA system is granted to members of the police whose personal details are provided to DoHA for registration. If inadequate number of the police is registered, information backlog might occur as few police officials would have access rights to DoHA system.

4.3.12 Automated access as an enabler to crime reduction

Even though automated access to fingerprint personal identification information that is based on complete fingerprints of the whole human set of ten fingers at DoHA is done by DoHA personnel, they instantly provide the identification details to the police officers that are residing in adjacent offices. Where the information is also expedited by the police to reach its destination of crime solving or court testimonies for instance, automation becomes and enabler to crime operations. According to Intell01:

…automated access is an important requirement for effective crime operations as it can enable us to be faster than the criminals. This is because once we know their identities or if we are in possession of their fingerprints, this would mean instant access to any piece of their identification details which can equip us to act swiftly and block them from any further communication with others. Automated access to information can provide us with the element of surprise to act swiftly before the criminals outpace us. This is because when the suspects become aware of our progress in the investigations about them, and they get to know that they have been identified and that we are on their tracks, they cover their tracks well.

Automated and random access to information can ensure that the police can access personal details of suspects before the suspects become suspicious of being tailed and therefore provide the police intelligence operations with the edge over criminals. This will definitely make us to be quick and accurate through automated and sophisticated information gathering, processing and timely decision making to combat crime.

This can also allows easier information sharing amongst other units that can benefit from synergies of combined intelligence sharing as criminals operate at random and from all from various areas as they travel around. By sharing information the police from other regions can share details of modus operandi of certain criminals which can enable for more crime prevention and combating strategies. According to the police superintend from Centurion who is now an intelligence officer and was once when he was still a crime detective and was requested to assist in another area, he saw an operation style of safe crackers and was immediately aware of who the suspects were.

His knowledge of the modus operandi of the suspect was confirmed when the suspects were successfully convicted after being tracked and charged. He says that using ICT to access the database at DoHA can enable the police with Easier and faster access to personal identification details of suspects which can boost crime operations to provide the police with quick turn around times, faster courts hearings

and outcomes. Automated access to information by SAPS at DoHA would enable crime operations system to instantly and accurately identify suspects leading to faster legal arrests, releases or prosecutions criminals. The police can act swiftly and their planning can lead to instant accurate results since the identities of most or many suspects and criminals will not be mistaken.

4.4 The security policy requirements at SAPS

The police are expected to implement security measures on information in their possession and on information that is made available from DoHA and how it is protected while such information is in transit between DoHA and the police. This will also include information in transit between the police and the courts where it is used as evidence. The security of this information is a very important requirement of policy.

To achieve this, the police are expected to apply procedures that are in compliance with security requirements of policy and implement all security measures to ensure that possible manual or automated gathering, processing and storing of information is achieved without any security breaches. Both manual and automated access, by SAPS to information held by DoHA may help enable crime operations but this may also present challenges.

4.4.1 Manual access compliance

Manual documents of suspects and criminals' fingerprint records are securely filed in locked file cabinets and strong rooms that are protected by butler doors, windows and alarms. These offices containing the personal information and fingerprints as well as racks and cabinets containing the information are always locked where only authorized officers are in possession of keys that enable them to gain entry. Measures are also in place to ensure that information that is in transit between the LCRC and CCRC is protected. LCRCWO02 says that:

For security purposes, the CCRC in Pretoria only accepts fingerprints received from us as the LCRC or police stations from all provinces to ensure control over legally lifted fingerprints to be processed. Where matching prints are found at DoHA and

the suspect is found and charged, the personal details including the fingerprints are destroyed if the suspect is acquitted.

Various other officials in the CRC and the police station are in agreement that where arrested suspects are acquitted, their fingerprint identification details including those from DoHA are destroyed and not stored as measures of extending security against unauthorized access. The officials working and transporting the personal information and details are selected, security cleared and vetted. Information in offices or in transit is always in sealed protective containers and not exposed to potential unauthorized access. Only authorized officers are able to enter the system. According SilvCP01, "the authorizations, vetting and security clearances of officials are done as a requirement of, or in terms of section 212 of criminal procedure act 51 of 1977". He also reiterates what all others are continually repeating that the fingerprints are processed in room where unauthorized entries are prohibited.

4.4.2 Automated access compliance

The police are convinced that security is enhanced through ICT to protect the information from DoHA since in their own environment, the Automated Fingerprint Identification System and other crime operations systems are password driven and also verify the authenticity of officers that are authorized to operate the electronic system through biometric fingerprint identification process. The police system contains crime records of only the convicted criminals which are securely stored in the Automated Fingerprint Identification System (AFIS) database at the criminal record centre in Pretoria. Scanned fingerprints will also only be processed if the request contains all the authentication details which are always required.

Even if unauthorized officials with bad intentions do gain entry into the offices where the AFIS or the HANIS are operated from, security is still tight. DHADR01 says that:

Access to HANIS is restricted through various means. The system will perform a fingerprints identification or authentication which, if successful will prompt the user to enter their usernames and passwords where after it will perform the authorization

procedure before allowing anyone to access the system. The system knows everyone's user profile which contains controlled and predefined specified functions that can be carried out by the each user. Where the police are allowed access here at DoHA, there is no risk of security violation since they can only query to view identification information without any chance of deleting, updating or adding any record just like the controls included on ATM machines.

The authentication process ensures that security requirements are complied with even though some of the authorized officials are corrupt and have been reported to access the system and contaminate the information to undermine the crime operations. This revelation comes from various police officials.

4.4.3 Manual access procedures

Like the handling of all other manual documents, all documents with fingerprint details are securely locked in areas where unauthorized access is not allowed. Both the crime office and the LCRC process the fingerprints in private and secured offices and use sealed containers to store and transport them to and from the criminal record centers (CRC). All fingerprint related processes are done by security cleared and vetted police officials. The information regarding the fingerprints identification is only revealed when used by authorized investigating officers or at courts.

4.4.4 Automated access procedures

The equipment and applications or hardware and software systems respectively where the fingerprint processes are performed are safe guarded and access to the premises is restricted according to agreements with between SAPS and DoHA. Not all SAPS and DoHA personnel have access to these offices. The fingerprint identification information in DoHA is highly secured and access to information is also highly controlled.

The identification details on the SAPS officers' appointment cards should correspond with those on the registration list of authorized officers that is kept by DoHA to identify the police otherwise the requests will not be deemed valid by

DoHA who will not allow even authorized police officers to access their database management systems premises. Where officials are allowed access to systems database at DoHA fingerprint readers, user profiles and passwords are further security measures that are implemented to control access.

4.4.5 Challenges of manual access

The manual fingerprint process results in several trips being taken by the police officials between SAPS' central criminal record center and DoHA, or between central criminal record center and police stations or local criminal record centers which are located at certain police stations. This is due to mostly bad quality of the fingerprints lifted randomly from crime scenes. LCRCT01 raises his concerns around the possible security violation saying that:

The security of the information may be jeopardized as some of the prints face risks of being lost due to many trips between the two departments and internally between the criminal record centre and crime offices in all provinces. This is because of quality issues pertaining the latent fingerprint processing.

These prints are mostly returned unprocessed from either DoHA or CCRC. These have to be retaken several times in certain cases. The to and fro trips may jeopardize the security of the personal details being processed as some of the lost or misplaced prints could land in dangerous hands. Some officials may also bridge the security requirements through carelessness during the trips and confusion may arise while some officials can engage in corrupt activities with the criminals.

4.4.6 Challenges for automated access

Officials are cleared and their fingerprints are registered in the system as part of the user names and unique passwords. Such authorized officials and the skills required are sometimes scarce. This is due to the authorization procedures taking too long while ICT skills are not rive amongst police officers. Since the system will only allow registered, authorized and skilled personnel, this may be a problem.

4.4.7 Relevance of security policy to crime reduction

Security of personal identification fingerprint information is important to prevent any contamination of information by unauthorized users including those who may have the authority to access the information for viewing only. This is important to ensure that information remains reliable and accurate to reflect the true statue of citizens and others stored to assist the police by enhancing crime operations. The security of information is important for crime operations since protected information can be reliable, truthful and lead the police to take accurate steps in confronting suspects and criminals. If there are security breaches and information is randomly changed by unauthorized individuals for instance, police might chase wrong people with fake identification details or plan around wrong addresses that may lead them to stage intelligence driven cordon and search operations at wrong areas or places.

The police believe that if they can assure DoHA that they have implemented adequate security measures in place to protect their personal information, and if the DoHA security measures allow legal access which the police believe they subscribe to, then this will enable them to be able to rapidly identify more criminals at cordon and search operations which will contribute to the effective crime operations.

If information is protected against leakages to, or access by suspects, then the information will mostly be authentic and legitimate to effect correct planning and accurate representation to produce the right results like crime solving were suspects are positively identified or yielding fair outcomes of court verdicts.

4.4.8 Manual access as inhibiting crime reduction

The slow manual response is congesting the courts and slows the criminal investigation process. The other disadvantage may occur if access by SAPS, to information held by DoHA is denied. This can happen if, according to CCRC01:

…DoHA is not assured that we and other police members from the stations may fail to protect the personal details obtained from DoHA and we further fail to convince them that only authorized access will take place to use the personal information

solely for the specific purpose of identification, again, for security purposes, DoHA may deny access by SAPS to personal information in its possession.

He feels that DoHA may be justified in this case because:

…if there is lack of security to protect the information and therefore no proper access control, information can be deleted, wrongly updated or invalid new entries made to create a chaotic environment of unusable information that will mislead the police and may results in criminals being set free due to missing dockets or distorted evidence being presented.

CCRC01 also further explained that the success rates of finding matching personal details from DoHA are at the moment at very low level with regards to needed targets. He went on to explain the challenge as being, "due to lack of proper identification of latent fingerprints collected at scenes of crime which are sent to us by our colleagues from the police stations". Without security this could be worse where contaminated personal identification information here at DoHA may end up retrieving a woman's details when a man's fingerprints are scanned for instance. Lack of security can therefore completely inhibit on crime operations. This can also pose a serious threat to privacy concerns of citizens whose details could be randomly accessed by fraudsters.

The manual security processes take long due to protocol measures implemented where various levels of management have to attach their signatures on the application form SAPS to approve the retrieval of personal information which has to be given to the police. The latter wait long periods which renders their crime prevention strategies to be ineffective and inhibit on the police crime operations as well due to lack of information or information that is only available long after the damage has been caused. This could be through the freeing of detainees due to deadlines of detention period without charging the suspect while waiting for information from DoHA.

The requirements taken for privacy are the security measures that must be implemented. Information should always be locked up in offices that are accessed by

only authorized personnel. It should also only be processed and transported by authorized personnel. All authorized personnel are registered at DoHA. If there is a need from the SAPS side to increase production by increasing officers, the registration of new officers at DoHA might take long and inhibit crime operations due to backlog that might arise since unregistered SAPS personnel will not be able to access the DoHA offices.

4.4.9 Manual access as enabling crime reduction

This is already being addressed as seen by the current situation where both SAPS and DoHA are working together to exchanging information from adjacent offices in same buildings. Only the authorized officials from both departments have access into the premises or cabinets where details of personal information being dealt with are processed. The access control systems records the identification details of all authorized officers and DoHA employees who enter or leave through the access controlled doors and butlers of the offices and premises while any document changing hands between SAPS and DoHA personnel gets registered and signed for.

Secured premises containing sensitive information and records are accessed only by designated officials. The DoHA has built security measures around the personal identification information details database and also around how information is to be accessed exclusively by those who are authorized to do so. The police have implemented the same measures and are succeeding in building the same security which ensures that there is a seamless safe exchange between the two departments.

4.4.10 Overcoming automated access challenges

The security procedures applied for privacy requirements should be applied to protect information but to allow the SAPS necessary access for them to perform their crime prevention operations. Currently DoHA registers any police official identified as suitable to be included in the fingerprint identification process. Once registered, the SAPS official is provided with the user name and password to access the civil database from the designated offices adjacent to those of DoHA.

Wrong passwords could trigger alarms and disable access if entered persistently. The same levels of security built into the systems of the DoHA, and around its officials must be implemented in the police environment to ensure that information accessed securely reaches its destination. Charge and hold personnel accountable for the leaking of protected information that contains sensitive citizens' personal identification information. ICT should be made to record all transaction details including identifications of the transaction owners where non complying employees should be punished for leaking of information for instance.

4.5 The privacy requirements of policy at SAPS

All security measures that are implemented by both SAPS and DoHA to protect the personal information in their possession are aimed at the maintenance of privacy. In order to allay the concerns for privacy, certain procedures are implemented to overcome the challenges that are associated with unauthorized access to sensitive information. This has become necessary for SAPS to develop or adhere to access to information policies and procedures with specific reference to policy requirements for privacy.

4.5.1 Compliance of manual access

The police stations and the CRC's have implemented strict security measures where they use administrative clerks who are the custodians of keys for the strong rooms where the fingerprint documents are filed. Only they are allowed into these rooms. Even the police at their stations have to communicate through burglared doors when seeking information from these rooms. GarCP02 says that, "Since no unauthorized entry is allowed in the rooms where we store the files, no privacy violation will take place". By ensuring that only one person has access, this seems to enforce accountability on such a person.

4.5.2 Compliance of automated access

Where there is a security risk there is the potential of information leakages that may compromise the privacy of the fingerprint owners. Only qualified and authorized police officials can access information from AFIS as per security

measures implemented. The vetting of the officials also ensures that only trusted officials can access the personal information. These officials must are authorized and skilled to utilize the database management systems using password to access these system for instance.

4.5.3 Manual access procedures

SAPS follow procedures that ensure that no privacy of personal details owners are violated by restricting access to personal information to strong rooms and cabinets containing personal details only to authorized officers or clerks. The secured offices and selected officials ensure that unauthorized entry and access to information is blocked to comply with privacy. The procedures of keeping fingerprints with authorized investigating officers or handing them as evidence at courts ensures that the requirements of privacy is being complied with.

4.5.4 Automated access procedures

Where SAPS have been granted access at DoHA, they can only view information where they are allowed restricted and controlled access and only use printed information for either identification during investigations or at courts as agreed with DoHA. These control measures are implemented to minimize potential violation of privacy. Measures applied for security concerns are adequate to ensure protection of the privacy of citizens.

The security measures implemented through procedures for the authorization of officials ensure that the privacy concerns will be addressed by blocking unauthorized access where the ICT is used to preserve privacy of citizens using permitted access rights by users. The system complies with privacy by limiting access only to security cleared and vetted officers. Security also contributes positively to ensure that leakages do not occur to ensure that names or addresses of individuals involved in cases that can convict suspects or criminals are not leaked.

4.5.5 Challenges for manual access

Where there is a security risk there is the potential of information leakages that may compromise the privacy of the fingerprint owners. Privacy violation is at

stake in this case if the fingerprint details or personal information lands in the wrong hands. The corrupt officials may undermine privacy by leaking information to criminals. The challenges that are associated with contamination of scenes of crime or where fingerprints of wrong individuals are lifted from crime scenes with the results that confidential personal details of individuals who are unrelated to the crimes being investigate are retrieved poses a threat to the privacy of such innocent individuals.

4.5.6 Challenges for automated access

Even though the system complies with privacy by limiting access only to security cleared and vetted officers, the possibility of corrupt officials who are authorized to access the system may cause personal information to leak to third party criminals and undermine privacy of citizens. The tight security measures applied manually and by the database managements system of HANIS take privacy concerns into account.

Automation of access to information also enables remote access. This has a potential threat where hackers can remotely access the system to commit crimes like cyber crime. "The DoHA does not allow direct access through our computers because of fear that we might have uncontrolled and random access that could open their systems to abuse or leakages to the public", this is according to the police officer at the Central criminal record center in Pretoria.

4.5.7 Relevance to crime reduction

Security ensures privacy which can be problematic if not preserved. Wrong identification details can fall into wrong hands through negligence and may be used by criminals that fake their own identification details to commit cyber crimes, open bank accounts or access their victim's bank accounts *etc*. The rate of crime will increase if information details are randomly accessible by unauthorized personnel to violate privacy.

The first major problem that arises when sensitive personal information is randomly and unlawfully accessed and falling into wrong hands is individual privacy

violation. When individuals become married without their knowledge or wrong people know your addresses at random. Criminal activities may be committed and pointing police to wrong individuals whose identity documents are being used by criminals. This makes it difficult for crime operations which are directed by wrong information. Privacy has to be complied with to ensure that personal information from DoHA is accurate to enhance crime operations in the form of positive identification of suspects and criminals through their fingerprints where necessary.

The security measures, according to the police should convince DoHA that the police will comply with the privacy requirements. If their requirements of privacy also take into account the need for the police to access their database, then the protection of privacy by the police can contribute to effective crime operations. "The trust between the police and DoHA which has been destroyed by the corrupt behavior of some of our members can be restored if security and privacy concerns can be addressed by us when we process personal information that we obtained from DoHA", these are the words of the police officer at the Central criminal record center. The officer also says that DoHA had previously allowed them direct access to the civil database at DoHA remotely from the police central criminal record center through keying the identity numbers and retrieving personal details of suspects or criminals.

By complying with security and privacy requirement procedure, the police are hoping that the automated process could be restored and further strengthened to allow remote automated by SAPS to information held by DoHA which can comply with the accessibility requirement of policy to enhance crime operations. Information gathered against criminals will only be helpful if it is not known by the criminals meaning in this way complying with security and privacy requirements will enhance the police operations through improved crime operations applications. Security contributes positively to ensure that leakages do not occur to ensure that names or addresses of individuals involved in cases that can convict suspects or criminals are not leaked.

4.5.8 Manual access as inhibiting crime reduction

Violation of privacy results in more crimes being committed that relate to cyber-crimes where many unsuspecting citizens' details are illegally accessed and used in various fraudulent transactions like hire purchases, loans *etc*. SilvCP01 feels that maintenance of privacy ensures that information is not unlawfully altered but:

…while this process is important, the requirements to maintain privacy should not be too steep to hamper rapid access to information. The identification processes for the police by DoHA when the former enters the DoHA premises and at counters where the actual information from DoHA is received by the police officials should not be done in such a way that the times taken exceed that which is required before the successful prosecution of the suspects.

He argues that the privacy requirements can in this case work against crime operations.

If innocent citizens details are accessed by unauthorized personnel and randomly changed, criminals can change their identities, addresses etc. and the information would negate on and counter the possible success of crime operations when its intelligence is integrated with the fingerprint identification details form DoHA systems. Both SAPS and DoHA must protect the information from such access and ensure that only authorized personnel have predetermined access rights that will only allow approved access levels and that information being retrieved and exchanged does not leak to those who are not supposed to see it.

Potential witnesses or other stakeholders in crime operations or court procedures who pull out due to life threats from suspects or criminals who have become aware of them means that these criminals have invaded the privacy of the witnesses negative consequences. By violating the witnesses' privacy, crime operations will experience negative effect as criminals might walk free from prosecution as the results. If privacy is compromised, personal details of individuals fall in the wrong hands where witness details like addresses may be known by criminals who may kill them to stop them from testifying against them which may

result in a dangerous criminal evading jail term. CCRC01 believes that closer cooperation is the answer where:

…we have to understand their privacy requirements and demonstrate that we can comply otherwise they will deny access and this would be a barrier to crime operations as we need to identify everybody otherwise our crime operations will not be effective.

This is especially important for CCRC officials since the national fingerprints gateway from SAPS to DoHA is through CCRC in Pretoria. All police branches in all provinces submit their requests there from where they are given to DoHA personnel for processing. If few investigating officers around the country are not vetted and security cleared at the level required by DoHA, then the movement of documents between the two departments might bottleneck.

This is because SAPS understands that the privacy requirements at DoHA include that the sensitive personal identification information retrieved for SAPS should only be handled and transported by those appropriately cleared to minimize information leakage to unauthorized officials. Information from DoHA will also not be admissible in court unless signed by a DoHA director. The piling of processed documents waiting to be signed might act as barrier to crime operations whose success mostly depends on timely action by SAPS' intelligence officers.

4.5.9 Automated access as inhibiting crime reduction

Even though the automated access to fingerprint personal identification information of complete fingerprints at DoHA is done by DoHA personnel to ensure that no privacy violation occurs, the police do not have the authority to push the DoHA personnel for faster feedback. They regard this as inhibiting since it causes delays which undermine the police crime operations. Information has still to be delivered to reach the destinations in various provinces which further delay crime solving activities or court testimonies for instance. While automated access to information could improve the SAPS' system's reaction times CCRC01 also understand the possible concerns at DoHA and explains it as follows:

This might also create the impression of possible unauthorized access to information which DoHA personnel may be suspicious that even unauthorized individuals from elsewhere can remotely access the personal details and violate privacy if they allow us remote access:

CCRC01 also points to other various factors which he feels are restrictive to possible automation of access by SAPS to information held by DoHA when he further explains that:

If remote access can be granted without proper controls, this will increase the risk of privacy violation as there are hackers out there who train themselves with skills to disrupt other's information through remote access. We have to train our officials with DoHA systems to ensure that we all meet their requirements for privacy and security practices when we remotely sign on to their screens otherwise the damage that might result will cause more harm. This could result in our chances of tapping into the national identity system going up in smoke and impede our crime operations. Remote and automated access to HANIS can have the negative effects for privacy and crime operations in general.

Apart from the training needs identified by CCRC01 and various other officials, there are other requirements at DoHA that are general acknowledged by the SAPS. DoHA requires that all SAPS personnel should undergo security clearances up to the highest level before being considered for any possible access to the HANIS. This request, according to DHADR01 has been relaxed since the clearance procedures are said to take too long and would impact negatively if it was tightly applied as a strict access to information condition at DoHA. Should DoHA insist on this request, very few SAPS personnel will be provided with user names and passwords to access the DoHA's HANIS system. This would impact negatively on crime operations. Remote printing of documents by SAPS from DoHA will not be beneficial if the documents have to be manually signed by a DoHA director before they can be admitted as evidence in the courts. This would negate on the gains that

can be achieved by automated access and reduce the productivity level to that of the manual one.

4.5.10 Manual access privacy challenges for crime reduction

CCRC01 says that the concerns around manual access which are being echoed by most officers within SAPS are continually being addressed since they are in the process of subjecting their members to the necessary authorization procedures. The SAPS' and DoHA management are currently engaging in talks regarding the problem areas since crime, as he says is a problem to the entire country and not just to the police.

SilvCP01 says that, "all the authorized DoHA and police officials should be vetted and subjected to the highest level of security clearance related to top secret clearances which must be given priority and not be on waiting lists". This is because the general feeling is that only those officials including investigating officers and administrators that may have to legally access the information should be able to exchange information and be able to access it with minimal delay.

4.5.11 Automated access privacy challenges for crime reduction

CCRC01 is convinced that ICT has reliable security systems if proper controls and security applications are implemented. According to him:

…there is no chance that we can change the DoHA information in their systems since a user like me, or any of my colleagues who have been granted only viewing rights without any other capability where they can only view what is approved for them to view, can do any harm. This can be made to work just like an auto bank where one cannot change their bank balances.

According to most police officers, the authorized investigating officer for instance should only be able to view the personal identification details of only the prints' owner who is being investigated.

4.6 e-Governance developments at SAPS

SAPS, just like DoHA used to engage in manual fingerprint processing to identify suspects. This process has been in use for a very long time and required staff

at the Criminal Record Centre to physically compare fingerprints found on a scene of crime with the sets of hard copy fingerprints. This has led to SAPS introducing an e-governance initiative, the MorphoTouch which is a biometric fingerprinting tool that has revolutionized the way SAPS process criminal suspects. The system is deployed in various police sites countrywide. According to ITWeb (2007, in press) the system is used at roadblocks and during intelligence-driven cordon-and-search operations to link suspects with their crimes. In this way, a number of suspects including those who have eluded the police for prolonged periods of time have been arrested, prosecuted and sentenced after having been identified via the MorphoTouch.

The device was said to be housing about 50 000 fingerprints while it can be physically or remotely connected to the central police Automated Fingerprint Identification System (AFIS) database at the Central Criminal Record Center which houses copies of the fingerprints of over five million criminals. According to the ITWeb, The MorphoTouch can complete a local database query at operational areas like roadblocks for instance, within five seconds, while a search of the full database takes between five and 10 minutes depending on the network. Apart from the mentioned speed, the MorphoTouch is also claimed by ITWeb to be 98.5% accurate in the identification of fingerprints owners. The AFIS system is however only limited to criminal fingerprints in the police Criminal Record database while legislation prohibits automated access to personal fingerprint identification information in the civil databases like those held by the DoHA.

4.7 Background to DoHA environment

The findings presented in this chapter were collected from the organizational case study of the Department of Home Affairs (DoHA) in connection with the role played by policy in the process of access by the police, to information in their possession. While the database is utilized by the authorities at DoHA to fulfill their mandates of ensuring that citizens and visitors are registered, it can also be utilized for identification purposes. Since the citizens' database includes information of all perpetrators of crime, access by the police to this database has become important for

identifying the perpetrators of crime. While this measure has the potential to contribute positively to crime reduction, possible policy conflicts may arise.

4.8 DoHA services, related policies/legislation

DoHA authorities pursue their mandate of ensuring that every South African and visitors are appropriately registered and can be identified through their performance of civic and immigration services. The department has various offices in all provinces and in many regions within these provinces where the offices are mostly found in cities and smaller towns as well as in townships. Some cities have multiple office sites while the department has also organized mobile units to reach some of the underlying remote rural areas. DoHA strives to reach all citizens of South Africa and visiting foreigners including those that may wish for permanent citizenship, to work or do trade locally.

4.8.1 The civic and immigration services objectives and policy

According to the Constitution, the services performed by DoHA are divided into two broad categories, the Civic services and the Immigration services. These services are guided by related policy and legislation. The civic and immigration services are offered to citizens and foreigners respectively.

Some of the civic services include determining if citizens are eligible to be issued with identity, passport and travel documents or whether they qualify for social grants and other such benefits. The civic services are mostly enabled through the management of National Population Register (NPR) and the Home Affairs National Information System (HANIS). Both these databases contain the citizens' personal identification information such as names, identity numbers, sex statue, addresses *etc.* as well as birth, marriage and death records.

The immigration services include controlling the entry of foreigners into the country and determining their residency statue while managing the refugee affairs. Permit documents are also issued to the foreigners from the department for identity purposes and efficient management and regulation of migrations. DoHA thus uses the NPR and HANIS databases to acts as a sole custodian and the single national

point of verification of the statue of the identities of citizens or resident foreigners while securely storing these databases to contribute positively to the promotion of national security. The provision of immigration services projects a good global image for the republic.

By providing civic and immigration services locally and globally, the department attains other objectives of contributing significantly towards the national socio-economic development by ensuring that citizens and legal visitors have appropriate identification documents that enable them to access the benefits and opportunities in both the public and private domains.

DoHA officials are guided by various policies and relevant legislation in pursuing the objectives of ensuring that everybody, young or old are registered and can be uniquely identified through their identification numbers or fingerprints. To achieve this, the Identification policy and its related Identification act, No. 68 of 1997 as amended and the Regulation made in terms of this act serve as guidelines for compliance.

4.8.2 Citizens identification

The NPR is indexed by the identity number which is typed into the system to retrieve the unique personal identification details of the identity document holder. In contrast, HANIS can also be indexed by the fingerprints of both hands which if scanned into the system in the particular sequence in which the fingerprints were stored, retrieves the unique personal identification details of the prints' owner. The databases therefore compliments one another while they may be more useful than one another depending on what is available to use as key to search for personal identification details.

Since DoHA is the sole custodian of the national databases, it has become essential for officials from SAPS to have a need to access these databases for verifications and confirmations of identities of perpetrators of crimes in their investigations for crime prevention and combating operations.

Access by the police, to information held by DoHA takes place when the former submit the identity numbers or fingerprints belonging to the perpetrators of crimes to DoHA who keys the identity numbers into their system or scan the fingerprints to produce accurate personal identification details that are provided back to the police to enable them to take appropriate actions against suspects during their crime operations.

4.9 The accessibility requirements of policy at DoHA

The accessibility requirement of policy at the Department of Home Affairs (DoHA) is about how access by SAPS to information held by DoHA should be made possible and in accordance with policy. While e-governance programs that are being implemented can expedite this process by providing amongst others, easier, remote and faster ways of access by SAPS to information held by DoHA for instance, some challenges are emerging with the implementation of e-governance technologies which may be in conflict with both security and privacy policy requirements. This raises concerns that need to be taken into account.

4.9.1 Manual access compliance to Policy

DoHA has implemented strict information access control measures to ensure that the SAPS comply with the manual accessibility requirement of policy when requesting access to the fingerprint identification details in its possession. DHADR01 had this to say:

…we only provide the personal details of only the suspects that are being investigated since the police are required to furnish case details that are being investigated when they request fingerprint identification details. They have to do this in accordance with the agreements that are reached with them to ensure that they use the personal information from us strictly for specific identification and verification of the suspects being investigated.

According to DHAEX01:

…the police have made an undertaking to us through the relevant structures that they will never use the personal information from us for any other purpose except for

what it was acquired for as required by law. They are only given the matching personal information details for the fingerprints they submit to us and for which they provide our officials with the reasons which are always to do with crime as the main purpose.

DHAEX01 also say that for as long as the police' application requests for information are in compliance with the current protocol procedures of DOHA, then the latter will continue to cooperate with them. The other reason for cooperating with the police is that DoHA regards crime as an important issue which should be resolved by all citizens. They trust that the police will respect information policy since they are a public institution bound accordingly to comply.

The fingerprints on hardcopy prints contained in sealed envelopes are handed in only by registered and known SAPS officials to ensure that the accessibility of the identification details is controlled and only given to right people and for right reasons. The DoHA co-operates and makes sure that where possible, the personal information that is being legally required is provided in accordance with the agreements between the two departments.

4.9.2 Automated access compliance to policy

DHAEX02 believes in the accuracy of HANIS that will always be relied on to retrieve the correct details and not infringe on privacies by retrieving innocent details. He says that:

HANIS will never retrieve details of an individual who is not the owner of the fingerprints. When fingerprints are scanned into the computer, it only retrieves the matching personal details which DoHA is assured will be used only for the identification purposes and given to authorized SAPS officials.

He maintains that privacy will not be violated if fingerprints are used to retrieve any personal details.

4.9.3 Procedures for manual access

Even though DoHA has automated the fingerprint processing, there are manual processes that have to be followed prior to scanning the prints into the

computer. The DoHA personnel will only start the identification process after verifying and authenticating the approved application forms from SAPS for fingerprint identification of only complete prints (all ten fingerprints from both hands and clearly marked so that each fingerprint corresponds with its specific finger as stored in the HANIS).

Latent fingerprints or fingerprints uplifted from crime scenes cannot be positioned to indicate the position of the finger on the hand. This creates a challenge since the fingerprints cannot be used to instantly retrieve the details of the owner. The SAPS officials transacting with DoHA have to be registered and be in the list which is in the possession of DoHA. Once this has been cleared, there is a duplicate database, which is not live or active and from which the registered SAPS are allowed to perform the time consuming search based on one fingerprint. This process takes too long and does more often than once fail to produce the correct identification details.

4.9.4 Procedures for automated access

All requests for matching fingerprints follows the same authentication procedure before the actual prints from SAPS are scanned into the HANIS at DoHA. The HANIS is designed to do online verification by reading all ten fingerprints from both hands of an individual and retrieving the identification details of only the owner of the prints without exposing anybody else. This is the only information details provided to the police upon their presenting legitimately approved application for such details. This is also done on the assumption that SAPS will use such information strictly for the intended use of identifying the suspects or individuals for whom they have done such application.

4.9.5 Concerns for manual access

The process of retrieving personal fingerprint identification information for the police is not adequately helping them since most of the police queries are based on latent fingerprints which even if they are retrieved successfully, it still takes days to produce results. The DoHA is under resourced to provide optimal services to the

police. Their success rate of helping the police to identify criminals is still too low, according to DHADR01. DHAEX02 says that there are too many illegal immigrants whose personal identification details are not in the DoHA database system and therefore cannot be identified through the processing of the latent crime scene fingerprints.

Information from DoHA is that the request for personal identification information through fingerprints is only instantly successful if the individual is available in the system and all his or her ten fingerprints from both hands are not only available, but are aligned according to their positions on the hands which DHADR02 says is the only condition where HANIS instantly produces results. He also feels that the two departments have to work together and cooperate to ensure better results. This is because the illegal immigrant crime may be a police issue but it impacts on DoHA as well as it is trying to control the movement of all individuals into or out of the country.

DoHA feels that the other concern albeit of minor importance is that they have no control on how the personal information is used once it is in the possession of SAPS. While they trust SAPS, this does create some concerns even though they expect the police to abide by the regulations.

4.9.6 Concerns for automated access

In his own words, DHADR01 had this to say:

The DoHA systems were done in isolation and no considerations for other departments' systems interactions were taken into account. The HANIS system should be adapted to enable it to be productive to all police fingerprint identification requirements. Currently the system is only helping the police if they are in possession of all the ten individual fingerprints and positioned according to how they were captured into the HANIS system. The police's biggest challenge is the latent fingerprints that they lift from crime scenes.

The DHADR01 further explained that it is for this reason that the DoHA system, in its current form is not designed to adequately assist the police. He said

that too much money will be needed to upgrade the system and even then, good co-operations starting at the political level is needed which is not currently visible. Cyber and fake identity crimes are still high due to too many undocumented immigrants. He felt that some of the crimes are committed by the police like losing information for instance, leaking it to criminals is also seriously on the high. DHADR01 further argues that the system on its own will not be effective for current crime wave which he suggests that the system should be augmented with DNA capabilities to add more evidence needed to link suspects with crime.

HANIS works successfully when all ten fingers are scanned. The need to identify owners of latent incomplete fingerprints collected from scenes of crime is the most important for crime operations as this is the one issue that would greatly help the police. DHADR02 confirms the concerns being raised and says that the technical design and capability of the retrieval criteria of HANIS is incompatible with the way the police request information from DoHA and hence the latter's failure to enhance crime operations. He also re-emphasized the need for a major upgrade if the system was to be enabled to improve the police searches for identification details. He was not only concerned with the police for possible privacy violation as he said that even their own officials can commit cyber crime by bridging security and leaking information with harmful results.

4.9.7 Relevance of access to crime reduction

The DoHA employees agree that access to identification information will increase the success rate of crime operations. DHADR01 explained that lots of crime takes place against many departments resulting in loss of billions of rand as seen by housing and social grants being fraudulently obtained by non deserving individuals including illegal immigrants while the waiting lists of houses for citizens are growing by day. "These crimes could be greatly reduced if all the departments were co-operating and all were able to access the fingerprints identification details from DoHA to accurately validate all individuals before they provided them with services", DHADR01 further argues. The participants felt mostly felt that legal

access to fingerprint identification personal information at DoHA is vital to crime operations to prevent and resolve crime issues.

Like all other participants, DHAEX02 says that since DoHA is the only department with the civil database and HANIS that also contains images of photos and fingerprints, this makes DoHA central to crime resolution through accurate identification but according to him:

The resolution of crime is the responsibility of all citizens, departments and institutions. It is also the responsibility of DoHA to contribute to the combating of crime. The one way that DoHA can contribute to crime operations is by ensuring that any information in its possession is legally being made available to the police as and when it is needed as long as the process is controlled and not abused.

The DoHA views automated access to its database by SAPS as enhancing to crime operations which can definitely be boosted by automated timely identification information to reduce uncertainties during crime operations and courts. This is also due to access to personal information by SAPS at DoHA being necessary to also addressing crimes that affect DoHA which relate to entry into the country by illegal immigrants or undocumented migrants. DoHA also feels that access to their databases should also be extended to other departments like the South African National Defense Force at borderline operations or at ports of entry.

4.9.8 Access as inhibiting crime operations

Lack of communication, trust, and believe that SAPS would use the information strictly in accordance with the agreed conditions to safely secure personal information obtained from DoHA and thereby preserving privacy of individuals could lead to access to personal identification information from DoHA to be made more difficult and could compromise on the data gathering from DoHA and hence on the possible success of crime operations.

4.9.9 Manual access as a barrier to crime reduction

Manual access causes delays as most fingerprints uplifted randomly are damaged and there are lots of repeated attempts before unique matching prints are

retrieved. This delays the prosecutions and police programs as sometimes accurate matching prints are not easily identified and mistakes can be made.

4.9.10 Manual access an enabler to crime reduction

The DoHA is certain that where matching prints are found and these are given to the applying police officials, the information details are mostly very helpful to SAPS and serve to enhance their crime operations activities. The fingerprint services are now done on the ICT system and manual comparison is not done anymore.

4.9.11 Automated access as a barrier to crime reduction

Where identification based on fingerprints which are randomly collected at scenes of crime is requested by the police, DHAEX02 says that:

The DoHA system is not designed to verify that way and it takes long times to find random matching prints as searches are done (one to many) where a one fingerprints are scanned and have to perform search against millions of prints. This consumes the system resources and inhibit on other day to day processes of identity documents and passports. Our relevant units have created a duplicate database which is specifically created and is separately searched and takes several days at times to find a match and in many instances the search operation is not successful.

In this regard, he feels that HANIS may not contribute positively to crime operations.

The current agreements are that only DoHA personnel can sign onto the HANIS system and are co-operating with the police who sit in adjacent rooms but same DoHA buildings and provide instant details of all legal request of complete fingerprints searches. This may create a bottleneck since this is the only national police gateway to DoHA fingerprint identification process. Security and privacy violations could be the concerns of DoHA and thereby rendering automated access to be a barrier to crime operations. Automated access can provide fast information gathering, processing and quick decision making required by crime operations

systems and therefore it‘s non-implementation would be a major barrier to effective crime operations.

Several employees at DoHA are unanimous that the police deserve their cooperation but they stress that even though the automated access enables easy and fast information exchange by internet or email for instance it may also pose risks of unauthorized access by hackers. They do believe that ICT can be trusted to be properly controlled through firewall applications for instance and other uses such as the biometric authentication passwords must at all times be enforced. They also suggest that great care by those who are authorized should be taken to avoid passwords for instance from falling into wrong hands and resulting in damaging effects on both DoHA and crime operations. This is because hackers, as they say, may access the system and corrupt information or criminals may get access to know identities and photos of police informers or witnesses.

Opening the electronic databases for remote automated access over the wide area network also means possible opening for hackers who would try to access. Where “sign on” details falls in the hands of such users and they can remotely access the system with devastating consequences for DoHA and crime operations where such information is needed to combat crime. This type of access should only be restricted to selected few officials who are cleared with the highest security level by NIA.

4.9.12 Automated access as an enabler to crime reduction

DHACO02 is a consultant that works for the private company that is involved with the development and implementation of HANIS and he had this to say: *Technology adds value to information by making it timely available. Easy, fast and accurate automated access to DoHA database will be a plus for crime operations that will combine the criminal record information with the instantaneous random personal identification information details from DoHA to identify many more criminals who will have nowhere to hide. Any remote link by the police could pave the way for unlimited pool of resourceful information that is available in various*

forms and images. The police can view the faces of suspects, names and addresses by entering the suspects' identification numbers and most importantly, their fingerprints then the police will be swift in their actions to bring the crime levels down.

Most DoHA participants share this view and agree that during the period when the police were linked and could remotely retrieve the identification details of suspects from DoHA, they were responding faster to cases where the identification details were important. The police needed to at least be in possession of the identity number to be able to achieve this.

4.10 The requirements of the security policy at DoHA

The Department of Home Affairs (DoHA) is expected to implement security measures on information in its possession and on how information is made available and used by external recipients like SAPS and other department. This is a requirement of policy which DoHA also expects SAPS to abide by. To succeed in the implementation of these security measures, DoHA applies procedures that are aimed at protecting both manual and possible automated access to information in its possession to comply with security policy. Both manual and automated access, by SAPS to information held by DoHA may help enable crime operations but they also present challenges that raise security concerns if they are not taken into account.

4.10.1 Compliance of manual access

DHAEX02 is adamant that security measures at DoHA are implemented at all times during the communications between the two departments. The employees at DoHA and police officers involved follow certain procedures like being vetted. He says that more details on these can be found at the relevant offices. He says that the security measures are such that:

…information at DOHA is strictly protected and cannot randomly be accessed without following protocol procedures. I know from experience when I was still employed there that they apply strict control measures to ensure that access to information from their databases is done under strict security measures and that

information is protected and only made available to the applying police officials and is never leaked to any unauthorized personnel by us.

DHAEX02 says that even though he was not directly involved, he does know about how greatest care was taken to protect the information.

Entry to offices that are being used to process personal information is restricted to only the registered DoHA officials and the SAPS officers. According to the Director at DoHA fingerprint processing office, DoHA personnel are in possession of the register that contains the names and force numbers of all the police officials or police members that are authorized to bring or take the fingerprints detail information. These officials from the police are identified by their appointment cards that bear their identification details that include their names, identification numbers, force or Persal numbers as well as their facial photos.

4.10.2 Compliance of automated access

The system is not accessible by anybody including DoHA personnel who are not authorized. The details retrieved are only given to known authorized SAPS officials under agreements that the information will be protected at all costs. Several employees at DoHA have the confidence in the security provided by the computer system where access cards, usernames and passwords are used to control access to the system or databases.

4.10.3 Security procedures for manual access

Access cards are provided for entry into the premises and offices where sensitive information is being processed at all times. These checks are done upon entry and exit movement in and out of the DoHA premises for all individuals regardless of whether they are DoHA employees or the police officials. All internal or external authorized personnel have to make applications for the access cards while their fingerprints are scanned and registered in the biometrics systems at entry and exit points of the offices and premises. This is to ensure that the security requirements at DoHA are complied with.

4.10.4 Security procedures for automated access

Various security procedures are followed to comply with policy at DoHA. DHADR01 explains some of them as follows:

Access to HANIS is restricted through various means. Fingerprints identification and authentication will prompt the user to enter user names and passwords of approved officers allowed to access the systems. Within each user profiles, there are controlled predefined specified functions that can be carried out by any user. Where the police are allowed access, there is no risk of security violation since they can only query to view identification information without any chance of deleting, updating or adding any record just like the controls included on ATM machines.

This echoes the confidence which various participants have on the security around the database at DoHA. This was also corroborated by DHACO01 when saying that, "the only way an unauthorized individual to fraudulently access the HANIS is to do what criminals do with the ATM's to access and steal money from the machines". He goes on to say that they can only achieve this by, "by bombing it". DHADR02 confirmed what DHADR01 and the police officials had told the researcher when explaining about the security procedures of automated access by saying:

…the authorized police used to be granted restricted access rights to the National Population Register (NPR) database system that enabled them to only retrieve identification details by entering or keying ID numbers of the suspects for instance to instantly identifying or verifying the suspect's identification details. The HANIS is only accessed by DoHA personnel who co-operate with and work together with the police sitting in adjacent offices to expedite the fingerprint identification process. The various levels of access rights to both databases are to ensure that information can never be contaminated since rights that enable users to change, delete or add information are restricted to only those who are authorized to do so.

DHADR02 and DHACO01 also both further explained that once a user is identified and tasks are allocated to him or her, access rights that are relevant to such

tasks are built in the users' profiles and each time such a users "sign on" to the system, the system sets up how the user will access it and will never permit such users to do anything else other than that being prescribed in their profiles.

4.10.5 Security concerns for manual access

Various concerns are being raised around the authorization procedures which the police are required to undergo to be eligible to deal with the sensitive personal information at DoHA. DHADR01 shows that some of the procedures may actually work against crime operations even though this would not be the DoHA's fault. He says that:

…even though the police officials have to be vetted and security cleared to gain trustworthiness from us so as we can believe that our information in their possession will be safely stored and used, the process of vetting and clearances are done by NIA and these takes too long to complete where the waiting list stays high. The police officials are hired and begin to work while waiting for clearances which are completed long after they have gained too much experience in their work to be expelled if their results came out negative. This may result in unsuitable officials being kept in employment and dealing with sensitive information and can pose security risks.

DHADR01 says that this is the reason DoHA has relaxed in some cases, the requirements of authorization of police officials to enable continuity while the authorization waiting queues are being addressed. The current security measures are adequate and there should not be any security bridges unless vetted and security cleared officers commit frauds.

4.10.6 Security concerns for automated access

Even though the security systems are in place it will not help if crime is done from inside by those who should be preventing it to renders the security systems ineffective. This is because the system is adequately equipped with security measures to ensure that only those permitted to access can actually do so in accordance with their allowable functions. "There are no concerns with regards to

our security as the physical access is highly restrictive and the access rights to the NPR and HANIS cannot be easily bypassed unlawfully", says DHADR02.

Some officials felt that cyber crime can be committed even by vetted officials from both the DoHA and the SAPS therefore none of the officials should point fingers at others. The DoHA officials who are saying this say that they do not have any concern for the police either being provided with the information or being allowed access to retrieve.

4.10.7 Relevance of security to crime reduction

DHAEX02 and DHADR01 believe that personal identification information should be provided to SAPS as and when it is required. DHADR01 further explained that it was unfortunate that the system at DoHA was not designed to be more helpful to the police than what it was currently designed to do. But the information was definitely required by the police to provide the services to the community which makes this the responsibility of DoHA as well.

He further says that the provision of information to SAPS should not be done at the expense of security considerations which have to be taken into account with specific reference to addressing privacy concerns. Security measures being implemented should ensures that sensitive personal identification information, which can be harmful if leaked to wrong individuals like criminals, is protected. Names or addresses of potential witnesses may land in the hands of criminals who might pose danger to the safety of such individuals if strict security measures are not applied around such information.

4.10.8 Manual access as inhibiting crime reduction

The security requirements of policy may inhibit crime operations if not properly set up to ensure smooth operations during manual access by SAPS, to information held by DoHA. SAPS may be the reason at times for this challenge. DHAEX01 explains it as follows:

If the SAPS do not apply adequate security measures to personal information acquired from DoHA, leakages of sensitive personal details would result in the

outcry from the citizens at large and this would put pressure on DoHA not to easily release the information which would hinder the crime operations programs since only DoHA possesses the national personal fingerprint identification information.

DHAEX01 emphasizes how important it is for both departments to comply to security requirements as the public has the vested interest in how their personal information is being processed. This also highlights how non-compliance by SAPS can inhibit crime operations.

The participants at DoHA understand that compliance to privacy at their department is about innocent citizens' personal information being protected against illegal access. If security measure as per policy are not properly implemented by SAPS to protect the information during manual access where physical envelopes containing fingerprints details are transported hence and forth between the two departments, then DoHA firstly will not release such information which will have devastating consequences for crime operations as access will be denied.

If there is privacy violation then there will be an outcry from the community who will call for stricter security measure around their personal information to be implemented and these measures might include tighter protocol procedures that will further delay the exchange of information between SAPS and DoHA. Again this will work against the timely access by SAPS, to information at DoHA and hence work as a barrier to crime operations. DHADR02 explains that:

…the security procedure requires the Director General at DoHA to follow an authentication protocol procedure to physically sign the forms that contains the personal details received from DoHA by SAPS before these can be accepted as valid evidence by the magistrates at the courts.

While this manual process is a requirement for security purposes, it also unfortunately seems to undermine the processes for crime operations due to it being too slow for the process of access by SAPS to information held by DoHA. This would inhibit crime operations and impede on efforts that aim for instant

identification of suspects for positively linking them with their photos or fingerprints for prompt action.

4.10.9 Automated access as inhibiting crime reduction

The senior management at DoHA is in unison where access by SAPS, to information held by DoHA is concerned. This has to be achieved at all costs but the ball is always thrown at SAPS to ensure that the process is successful. DHAEX02 for instance, is not wavering in the trust he has on DoHA to always comply with the security requirements. But whether SAPS will successfully continue with this process, is in the hands of the police. He says that:

…if the security measures are not adequately implemented by SAPS during access and transmission of information to their areas where this is needed for their crime combating and prevention operations, or if because of this, information is accessed by hackers who have only bad intentions for instance, privacies of citizens would be at stake. If this can happen, the citizens would be up in arms and will make calls for the external automated access to information at DoHA by SAPS and other departments to be stopped. In this way, automation of access by SAPS, to information at DoHA would be in conflict with the security policies and will be the cause for the process to be stopped and pose as an inhibiting factor.

He said that under the circumstances then it can correctly be said that the automation of access to information is acting as the inhibitor to crime operations despite the automation having the potential to greatly benefit the process. Most participants at DoHA echoes the sentiments that as long as controls are not implemented to permit only legal access to information, the threat of leakages will result in automated access not being secured and safe and thereby negating on implementation of effective crime operations.

Skills are also raised as challenges that can render the automation process as inhibiting to crime operations. DHAEX01believes that:

Since only security cleared and vetted police officials are eligible to access the premises and the DoHA systems, therefore should these officials not have the

necessary technical skills required to understand the DoHA applications, this could negate on automated access which can in turn inhibit on crime operations. This can also have the same effects if the trained and skilled officials commit security breaches and are removed from the system. The system at DoHA works different from the SAPS' system which requires intense training for SAPS officials to make sense of.

This, as he further explains, calls for the two departments to cooperate in various ways to ensuring that they maximize the benefits that can be offered by the interactions of their systems.

4.10.10 Manual access concerns for crime operations

As in privacy concerns, authentication measures must be in place but with minimum process delays performed by vetted and security cleared officials from both SAPS and DoHA who are sworn to secrecy. The cabinets or any other container of personal information and details from offices or in transit between SAPS and DoHA offices must be sealed with auditable registered seals. Buildings must be physically secured and guarded to ensure that information is not contaminated or damaged so that it can be useful to crime operations.

The authorized officials must open and process the personal information documents only in locked offices where unauthorized officials are not allowed to enter. The document containers must be sealed and seals registered before they can be taken out of the offices for transportation between departments. Authorized SAPS and DoHA personnel have to know one another and work closer together. They must all be security cleared, vetted and sworn to secrecy by signing confidentiality clauses. Information being exchanged between the two departments must always be enclosed in containers with registered seals that have number tags. All officials must sign for removing and returning personal information documents being processed.

4.10.11 Automated access concerns for crime operations

The biometric fingerprint identification to authenticate the user accessing the computer system must be part of the passwords and the Persal or identification

numbers serving as user names to identify any authorized user before allowing automated local or remote access. It is correct, according to DoHA participants to allow both authorized SAPS and DoHA officials to share buildings albeit in different offices to exchange information to ensure that it always lands in the designated personnel. This would enable fast legal automated access to enhance the police intelligence operations and the courts. The systems must always be secured and no illegal entrants should be allowed in the buildings housing the offices mentioned.

The participants feel strongly about physical security of premises as well. They indicate this when some of them mention that even though the ICT systems responsible for the fingerprint processing require passwords for access, the equipment must still not be physically accessible by any unauthorized officials who, where possible, must also not see them. The necessary protection software must be used to only allow those who are allowed to access the system locally or remotely.

4.11 The privacy requirements of policy at DoHA

The privacy concerns at DoHA are the primary reason why security measures are being implemented. While it is easier to implement internal security to protect the department's databases, privacy of information that is being made available and shared with external departments like SAPS is still a big concern for DoHA even though it is virtually impossible to control the security measures over such information once it is no longer in their possession.

DoHA can therefore only rely on trust that other departments who are also subjected to and should be in compliance with the requirements of information policy to use personal information in accordance with the relevant laws. The department has also therefore made certain requests for SAPS for instance, which is one of the departments that is allowed access to information at DoHA to follow certain procedures for access to its information to minimize the concerns of privacy that may be aggravated by the possible implementation of remote automation of access by SAPS, to information in its possession.

4.11.1 Compliance of manual access

DoHA restricts information to ensure that it never lands in wrong hands except into those of authorized police officials or of its employees for instance. DHAEX02 explains this as follows:

Only SAPS personnel who have applied for fingerprint identification information and where approved to receive such information from DoHA are allowed access to such information after authenticating their identification and clearing their requests after thorough verification.

The participants at DoHA are unanimous on the safety of the information as they share similar feeling about the utilization of trusted individuals who must be authorized from both their department and the police as being aimed at ensuring that the process of the enquiry is legal and that only the relevant personal information being requested is retrieved, protected from falling into wrong hands and exchanged with authorized police officials to comply with the requirements of privacy. No one is allowed to enter the offices in which citizens' personal identification information is stored unless such individuals are authorized.

4.11.2 Compliance of automated access

Only authorized personnel possesses access cards or their fingerprints are authenticated by the system to enable only authorized personnel to access the information from the National Population Register (NPR) or Home Affairs National Information System (HANIS). DHAEX02 explained his staff used to comply with procedures for ease of use of the automated environment as follows:

If a correct identification number is typed in the computer that manages the database management system for the NPR or a fingerprints are scanned into the HANIS, then the accurate matching personal identification information of the owner of the identification number or of the fingerprints respectively is retrieved with minimal efforts.

He how ever immediately reminds the researcher of the concept of "*garbage in, garbage out*", which he says that this was at minimal levels at DoHA as they perform occasional verification processes.

4.11.3 Manual access procedures

DHADR02 explains that manual access to information procedures that are followed by employees and other external individuals like the police when applying for, or are being granted permission to receive personal identification information from their department are as follows:

The authorization procedure that is being followed by officials through vetting for instance is aimed at ensuring that only allowed officials can gain access to and use information from us. The fingerprint identification information at here is only made accessible to authorized personnel to avoid violations of the privacy of the nation at large. Once information is in the hands of police it is up to them to maintain our trust to protect the information for the future co-operation between the two departments. Our relationship should be based on trust and understanding.

It is with this understanding that the police receive and use personal information from DoHA in accordance with the legal purposes for which the information was requested. This is according to the DHADR01 who further added to his subordinate's authorization procedure comments that the security measures are aimed at preserving the privacy concerns in the environment that is only permitting authorized access to personal information.

4.11.4 Automated access procedure

While the DoHA participants are convinced that the "computer" as they occasionally refer to the keyboards and screens at their tables, will not allow any individual to gain entry to its system without been granted permission, DHACO01, who is the consultant from the private company explains this in a more technical jargon and says:

…the user profile of each user is issued with access rights that are granted to such a user to determine the transaction type that is permissible on each of all the records

in the database. These transaction types are, amongst others, "delete", "remove", "add", "save" and "change" or "modify" a record. Each user's transaction in the database is based on this user authority levels. No one can perform any transaction using their designated user-names and passwords which is outside what their granted rights stipulate. It is for this reason that you see cashiers calling their superiors to change something in the systems if they have committed errors or if they want to reverse a certain transaction because their user profiles only allow them to "add" money and not to change any transaction that had completed its execution. Our client's systems are also built on the same access control levels which allows those with more seniority to perform certain transactions which only they can perform at that level because they have been granted with relevant access rights to do so. A fraudulent transaction may be performed by a junior employee or police official if the get hold of their senior's user-names and passwords to gain entry into the system. This is also what the hackers are known to be doing at other people's systems without permission.

DHADR02 also added his voice to the procedures of automated access by explaining that during investigations of cases for instance where an individual's details are not correctly captured in the system as shown in their identification documents, once the concerns were validated and the details in the HANIS needs to be changed, even he could not effect the changes. He has to make recommendations to those who have the authority in the system to effect the changes and correct the details of the citizens directly.

4.11.5 Concerns regarding manual access

The participants at DoHA argue that from their side the security protocols are observed by employees who have all been vetted and security cleared. They believe that if ever the privacy of citizens and the nation at large can be at risk, this can come from the side of the cops as they say that compliance to privacy is dependent on the security provided by cops on the information once it is removed from DoHA site.

The officials and police who are not cleared according to security requirements may not be suitable for handling sensitive personal information that the DoHA is exchanging with the police. This, as they go on to elaborate, may result in leakages that will violate privacy. *"Privacy should not be violated if we stick to current procedures and requirements. If we can do that then information can be safely and securely exchanged"*, said DHADR02.

4.11.6 Concerns regarding automated access

The system is programmed to restrict access to only those security cleared and vetted officers, if these officials abides by the law, the requirements for non disclosure and the secrecy of information will be complied with and no violation of privacy through information leakages will occur. DHACO01 explains the automation challenges that may raise concern for the safety of the information in transit:

The tight security measures implemented into the database managements system that runs the HANIS does not necessarily guarantee that there will be no unauthorized access as this is totally dependent on those with the authority to keep their passwords safely protected from wrong hands. Opening the system to enable and allow remote access over the network is like anyone walking out of their house to walk in the risky and rough streets at night where possible criminals are roaming around. Even though one is armed for protection against the criminal elements, the safety of being armed is still not as safer as when one is safely locked in their houses. Information in the databases that do not permit external access is safer than when it is in the server that permit external access, or worse still, when it is in transit over the network between its destinations where various risks and threats of landing in wrong hands are more on the increase even though there are security measures in place for network transmissions.

The departments will however have to make do with the network security as information has to be shared to overcome crime. Unfortunately the commitment of DoHA personnel to serve the police and stop crime in its tracks through remote

transmission is just a dream since the DHADR01 says that their systems and those of the SAPS are not technically compatible to achieve such automated access.

4.11.7 Relevance of privacy to crime operations

The participants agree that the security measures are implemented to ensure that the privacy requirements which can be problematic if not preserved are upheld. Wrong identification details falling into wrong hands can be stolen and used by criminals that fake their details for cyber crimes, open bank accounts or access their individual's bank accounts *etc*. The rate of crime will increase if information details are randomly accessible by unauthorized personnel to violate privacy. Security is necessary to avoid any violation of privacy where an innocent individual may become arrested due to their details being used by criminals while they, as victims are innocent. This therefore according to most participants means that if the requirements of privacy are respected then crime operations systems will be accurate when the police access information at DoHA.

4.11.8 Manual access as inhibiting the identification process

The violation of privacy is the results of lack of adequate security measures and this will have the same negative results as with lack of security. According to DHADR02, the verification process and the protocol procedures aimed at compliance to privacy may be necessary but they consume a lot of time before the personal identification information is retrieved to reach its destination at various police stations or courts. Other destinations may be crime information offices stationed in the premises of the police stations in various regions or at the local criminal record centers which are also located in the police stationed in the regions of all provinces. This process inhibits on the effectiveness of crime operations.

4.11.9 Automated access as inhibiting the identification process

DHADR01 explained how privacy policy requirements for automated access to information might derail crime operations:

We perform instant retrieval of personal identification details for the owner of all ten fingers' fingerprints that are scanned simultaneously from HANIS and this is the

only time we are satisfied that only the real owners' details will be retrieved without including those of other individuals to violate their privacies due to them being innocent in this case. But where latent fingerprints which are not always visible and are drawn randomly from crime scenes which results in them sometimes retrieving wrong details, these are viewed as being in violation of the privacies of the owners of the wrong personal details that are retrieved. This has resulted in very restrictive control measures being implemented for privacy concerns on the automated access process done through the latent fingerprint searches. Even though the latent fingerprint searches, which are the instances where one fingerprint is compared with all South African's ten fingers (a one to many search) is an automated process, these searches take too long with inhibiting implications for the police crime operations.

While the biggest challenges for the police is to identify the owners of the fingerprints that are collected from crime scenes, the system at DoHA according to the DHADR01 was not designed to perform searches based on individual and isolated fingerprints

4.11.10 Concerns regarding manual access for crime reduction

The Director points out that DoHA requires all police members being identified to be registered at DoHA for the processing of fingerprint identifications to be security cleared even though this requirement is relaxed to allow the minimum delays in the processes. This he says is because the process of vetting takes too long. He also said that the police should prioritize the clearance processes so that DoHA could provide automated access rights to the civil database for the police.

4.11.11 Concerns regarding automated access for crime operations

The user names and passwords should clearly identify the officers accessing the system and should store the transaction details of officers for accountability. The SAPS personnel can be subjected to the same authorization procedures required to be performed on DoHA personnel to exclude those that are unauthorized from accessing the systems to ensure that only legal access to the systems is achieved for privacy of

information. Anybody taking a shift should be allocated identifications that will point all transactions to specific individuals.

4.12 Citizen identification process

In order to protect the identities of citizens, the personal identification details of the citizens are stored in the National Population Register (NPR) and the Home Affairs National Identification System (HANIS), which identifies individuals through their fingerprints. DoHA performs the civic services which include the recording of personal particulars with a view to issuing identity documents (IDs) to enable unique identification through identity numbers and by means of fingerprints and photographs to confirm identities once details are retrieved.

By being able to identify everybody through their identification numbers and fingerprints, DoHA is also able to serve other departments that need to verify and authenticate the identities of their clients like SAPS in particular who always have a need for accurately identifying suspects in their crime combating and prevention operations. SAPS submits the identification numbers or fingerprints of suspects to DoHA who keys the identity numbers into their system or scan the fingerprints to produce accurate personal identification details that are provided to the police to enable them to take correct actions against suspects during their crime operations.

4.13 e-Governance developments

Traditionally, the fingerprint authentication at DoHA used to be a manual legacy paper system process of checking which was consuming a lot of time while it was also according to the HANIS Website not very accurate and was unmanageable. This is due to the manual database becoming too large with time as the volume of files continued to grow and hence became unmanageable. To overcome these challenges, DoHA engaged a third party supplier company, NEC which introduced the Home Affairs National Identification System (HANIS) which is the world's largest civilian fingerprint identification database that has provided DoHA with a fully integrated 10 fingerprint identity solution to cater for over 50 million adults citizens in South Africa (HANIS, no date).

HANIS is a digital database that implemented a one to many (1:n) search database as the system's core ICT to ensures that every single new and existing fingerprint could be properly processed, verified and is accessible in real time with the accuracy rates of more than 99.9%. This is according to the Website which also states that the system's capability has also ensured that the database records which are in excess of 30 million are now digitally and securely stored in the database while the search engine demonstrates a significant improvement in accuracy. The Website further explains that HANIS is currently capable of storing and searching up to 50 million records.

4.14 Chapter summary and overview of the next chapter

Data was successfully gathered from officials of SAPS and DoHA through semi-structured interviews which went well even though the police were mostly uneasy at sharing information about their operations with a stranger who claimed to be a student. The findings from both SAPS and DoHA are accordingly categorized into themes based on the units of analysis in the form of the requirements of policy being accessibility, security and privacy.

These findings will now be analyzed in the next chapter five.

CHAPTER FIVE: ANALYSIS OF POLICY

5.1 Introduction

The mandate of SAPS is to reduce crime hence they must always be able to identify all the perpetrators while that of DoHA is to ensure that all citizens and other persons in the country are properly registered and hence they must always be able to identify all citizens and visitors. This is therefore creating a very important overlap between the departments' mandates. Since information at DoHA is used to identify all citizens, this has necessitated a need for access by SAPS to information held by DoHA for the identification of perpetrators to benefit crime reduction efforts. This process has however met with challenges as it is currently manual and too slow for the police to be effective in the crime reduction operations.

This has led to the need for the implementation of e-governance to automate access by SAPS, to information held by DoHA. While this will overcome the challenges of the optimization of crime reduction operations, the automation may potentially compound the policy conflict that will raise the concerns relating to privacy to higher levels. Both departments are interested in an effective policy for the guidelines for developing e-governance to automate access by SAPS, to information held by DoHA which is needed for the identification of all perpetrators to enhance the crime reduction process.

5.1.1 SAPS crime reduction

South Africa is faced by high crime levels that threaten the safety of citizens. The country is rated amongst the high crime countries (SAPS, 2010). The police are continually devising means of reducing crime. One of the strategies they are applying to reduce crime is the identification of the perpetrators. Since some of the crimes being committed are detected and hence reduced as the results of police actions, the police are intensifying the current manual identification of perpetrators through fingerprints and have automated the fingerprint processing for rapid, accurate and remote identification of the perpetrators.

The automation of access to information held by government for the identification of perpetrators with the intention of reducing crime has become an international norm. Schiller (2006) provides an example of the Erlanger, Ky., police department that used manual operations. Once the officials there adopted automation of access to information and gained the necessary ICT operations knowledge, Schiller explains that the shared searchable crime databases and systems enabled the officials to identify perpetrators remotely from their patrol cars.

5.1.2 The process of identifying perpetrators

The police are currently performing the identification of perpetrators at two levels. The first level takes place internally where they identify a suspect who has a criminal record and hence they can retrieve the suspect's identification details from their databases through the suspect's fingerprints. The second level concerns the identification done at DoHA for a non convict suspect whose personal details do not exist in the police system's database. The latter level is manual and slow since the fingerprints have to be physically transported to and from DoHA offices from all police stations through the CCRC. This manual process is despite SAPS and DoHA having automated their internal fingerprint identification processes where SAPS and DoHA are able to identify convicted perpetrators and all citizens including visitors respectively.

5.1.2.1 Manual identification

The physical transportation of the fingerprints from police stations and CCRC as well as between the latter and DoHA takes too long over a period that is mostly longer than the detention limited set by the law. This undermines the crime reduction process of the police since the perpetrators have to be released within 48 working court hours of being detained if the police action depends on the identification of the perpetrators which is taking longer than the detention period.

5.1.2.2 Automated identification

The two departments have each implemented e-governance to automate their fingerprint identification functions which enables for instant identifications of

perpetrators and citizens at SAPS and DoHA respectively. The automation of access to information at SAPS is also limited to the identification of convicted perpetrators. Even though information policy enables and guides the process of access, by SAPS to information held by DoHA, e-governance is not implemented to automate access by SAPS, to information held by DoHA. Since such automation raises challenges of policy conflicts, it would be important for an enabling e-governance policy to be established.

5.2 Broad access to information policy

In order to balance the right of access to information held by government, the policy includes three requirements that must be complied with in order to enable access to information while catering for possible associated concerns. The accessibility requirement calls for the promotion of access to information held by the state while the second, the security requirement calls for the effective protection of information to comply with the third requirement that relate to the privacy of citizens.

Various initiatives that were undertaken for the formulation of access to information policy includes broad consultations of the stakeholders in government at various levels, a range of civil organizations and non-governmental organizations as well as the public in general participates.

5.3 Access to information legislation

Sections 32(1)(a) and 32(1)(b) of the Constitution provides that everyone has the right of access to any information held by the State and for the horizontal application of the right of access to information held by another person to everyone when that information is required for the exercise or protection of any rights respectively. The Constitution also calls for national legislation to be enacted to give effect to this right in section 32. The Promotion of Access to Information act, No. 2 of 2000 is thus the resulting national legislation that was enacted to give effect to this right in section 32 of the Constitution.

The Constitution also calls for the State to respect, protect, promote and fulfill at least all the rights in the Bill of Rights which include the right of everyone to privacy. The right of access to information held by a public or private body is therefore not absolute and may be limited to the extent that the limitations are reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom as contemplated in section 36 of the Constitution.

Section 30 of the Bill of Rights in the Constitution guarantees protection for every one against others and also guarantees the right of every one to communicate or be communicated to in the language of their choices. To ensure that this is possible, Section 6 of the Constitution identifies eleven official languages of South Africa.

5.4 e-Governance planning and developments

e-Governance initiatives in South Africa were taken at the highest level within government structures including the Presidency. The process also followed a wide consultative path where all government departments were represented together with Ngo's and the public in general. The development were driven by the attainment of the Vision 2014 which calls for the inclusive information where ICT is effectively utilized and harnessed to, amongst others, modernize the ICT infrastructure to deliver citizen centric services. This is according to the Presidential National Commission in the Information Society and Development Plan or ISAD Plan (PNC-ISAD, 2006).

5.5 e-Governance policy

One of the first initiatives for e-governance policy formulation was provided by the country's vision 2014 strategy in which South Africa is described as an inclusive information society where the government has modernized the ICT infrastructure to provide, amongst others, quality services to the communities. The e-governance policy initiatives is centrally coordinated by the Department of Public Service and Administration (DPSA) that consulted broadly throughout government stakeholders (GITO Council) and involved both non-government organizations and

civil society in general to launch a national IT policy framework (DPSA, 2001). This framework created the basis for the implementation of e-governance for the public institutions.

The DPSA policy framework contains recommendations that the policy makers should ensure that the e-government initiative should, amongst others, address the intra-governmental operations (G2G). The Framework also emphasizes that the implementation of ICT was to be done in phases. Since then, there have been various e-governance policy measures and efforts at various tiers of government that are aimed at utilizing ICT to improve operations which would facilitate better access and services to the communities.

5.6 Key aspects of public policy

The access to information policy addresses the rights of access to information held by government as well as the rights of everyone to privacy which requires adequate security measures to be implemented to protect citizens' personal information held by government. Some of the key aspects of policy which also plays a role in crime reduction are as follows: it enables access to information held by government: enhances crime reduction by enabling the identification of perpetrators: enables the identification of all citizens: determine the status of the information society of a country: require security to protect information and: requires privacy of citizens to be maintained.

5.7 The analysis of the findings

All the themes and sub-themes have been summarized and categorized according to the three requirements of policy being, accessibility, security and privacy as the main themes as well as how they affect crime reduction through their role on the implementation of e-governance.

5.7.1 The analysis of the accessibility requirements of policy

The accessibility requirement of policy requires access by a department, to information held by another department to be enabled. The requirement also calls for access to information to be properly controlled to ensure that it is used legally and

for the purposes for which access was granted. This research was therefore conducted to investigate if access by SAPS, to information held by DoHA was being allowed as per the requirement of this policy.

The findings reveal that DoHA does provide SAPS with the identification information under controlled and secure environment where the fingerprints or identity numbers of perpetrators are brought to DoHA offices by authorized personnel and physically handed over. The DoHA officials performs the fingerprint processing after authenticating each request to ensure adherence to legal requirements before feedback to the police. There is no specific period for the return of the feedback from DoHA since this, according to DoHA, depends on its own volume of daily work and that of SAPS. Both SAPS' and DoHA's officials have good communications and are committed to following access to information procedures where they were able to explain various methods and procedures. It also came to light that the pre-described procedures enabled the departments to successfully adhere to the requirements of accessibility policy.

It is clear from the findings that manual access to information has been posing some challenges such as taking too long to provide the evidence that are being awaited by the police for prosecution of suspects, for instance. This has for some times, in many cases failed, as further indicated by the findings, to contribute positively to the police' objectives especially during emergencies which negated on police operations. Where manual access to information is successfully utilized, it is found to be very helpful in assisting the police in the identification processes.

The findings also revealed that as far as the personal attitudes of DoHA employees are concerned, they have been mostly found to be in support of both manual and automated access, by SAPS to information held by DoHA as long as this is done in accordance with the policy requirements. A further revelation from the findings is that the police are abiding by the policy and procedures of the accessibility requirement of policy internally when they gather information, use and store it. This was also found to be the case when they obtain and process information

from DoHA which also processes information according to policy requirements as evidenced from the findings.

The findings also revealed that being in compliance to policy was not the only reason DoHA enabled SAPS to access its information. DoHA employees also understood how access, by SAPS to information in its possession was relevant to the success of crime operations. It was further revealed that DoHA understands that crime is a national priority that was to be tackled by all South Africans who should all support the police.

Since employees are not acting as barriers, and policy is neither inhibiting access to information while the concerns raised can be addressed by the utilization of authorized officials, the presented barriers of slow turn around feedback requires the implementation of e-governance. E-governance has the capability to enhance crime reduction by automating access by SAPS to information held by DoHA needed for rapid identification of perpetrators.

5.7.2 The analysis of the security requirements of policy

The security requirement of access to information policy requires adequate security measures to be implemented to protect information held by government or which is in transit between departments. This is to ensure that information is not used for unintended purposes. This research was therefore conducted to investigate if the security measures were being implemented as per the requirements of policy.

The findings reveal that both DoHA employees and the police officials are committed to following procedures where they were able to explain various methods and procedures which they have been following to adhere to requirements of security policy in terms of restricting physical access to fingerprints offices *etc*. The findings also revealed that SAPS have been subjected to manual access to information security procedures.

The findings reveal that both SAPS and DoHA have implemented security measures to protect personal identification information in their possession and in the processes during manual access, by SAPS to information held by DoHA. The

physical security measures being implemented were found to include but not limited to offices that are always locked and protected with steel burglar proofed doors and windows where entry is highly controlled. This has enabled both departments to ensure that information and evidence being provided at courts were credible and contributing to the court prosecutions.

This has been successfully implemented where sole office occupants were revealed to be the sole custodian of keys to such offices. It was further revealed that there were various procedures being followed by the departments to follow security policy requirements where DoHA employees and police officials have to be subjected to authorization procedures and being sworn to secrecy which has over the time been successfully implemented to ensure that information at both departments and in transit between them is always protected by trusted officials. According to the findings, these officials followed security procedures where each of them has to follow identification procedure before being allowed entry into offices containing sensitive documents or before being given such documents for which they sign. This has also enabled the police that are approaching the courts for the prosecution of suspects to produce reliable evidence that was not accessed and contaminated by unauthorized individuals.

The findings revealed that the departments have also implemented security measures to protect their electronic databases where access is controlled through various measures such as user profiles, passwords, access cards and biometric applications that read an individual's fingerprints to authenticate their identities for instance. It could be established that both departments were satisfied that security measures were necessary for the protection and reliability of the information in their database.

While the security requirements for SAPS at DoHA were suspected to be one of the obstacles of automated access by SAPS, to information held by DoHA, on the contrary, the findings reveal that the inadequacy of, or lack of security measures at SAPS needed to protect information retrieved from DoHA could impede crime

operations as this could be used by DoHA as the reason to block access, by SAPS to information held by DoHA.

Some concerns revealed are that the security of information can be jeopardized by the repeated trips between the SAPS and DoHA which are made for the same fingerprints that are mostly returned unprocessed by the Central criminal record centers to the Local criminal record centers or police stations due to bad quality of manual fingerprints. The security concerns for automated access to information is that the authorization process takes too long and that officials are trained with ICT skills before their results are returned. If these are returned negative and skilled officials have to be removed from classified operations, this will create problems as ICT skills are scarce.

The departments are both in compliance with the security measures being implemented and persons from both departments are constantly in communication and are aware of the risks associated with access to information. Under these conditions, since they are also aware of the security capabilities of e-governance applications, an effective and adaptive e-governance policy can be formulated to enable the implementation of e-governance to expedite crime operations. This can be achieved by utilizing it for the automation of access by SAPS, to information held by DoHA which is required to enhance the identification of perpetrators.

5.7.3 The analysis of the privacy requirements of policy

The privacy requirement of policy is about ensuring that information of private citizens held by government should always and only be accessible by authorized personnel who must not use it without the citizen's permission except for lawful purposes. This research was therefore conducted to investigate if privacy requirements were being complied with by SAPS and DoHA during access by SAPS, to information held by DoHA.

The findings reveal that both DoHA employees and the police officials are committed to following procedures where they were able to explain various methods and procedures which they have been following to adhere to requirements of privacy

policy. The findings also revealed that SAPS have been subjected to manual access to information privacy procedures. The police are also expected to adhere to the privacy policy requirements during automated access, by SAPS to information held by DoHA as a public institution.

The findings reveal that both SAPS and DoHA have implemented privacy measures to protect personal identification information in their possession and in the processes during manual access, by SAPS to information held by DoHA. The physical security measures being implemented such as offices that are always locked and protected with steel burglar proofed doors and windows where entry is highly controlled, is done mostly for the purposes of complying with the privacy requirements.

The burglared doors at entrances of buildings and offices are marked in bold letters that say, "No unauthorized access" which according to the findings are measures of security aimed at minimizing unauthorized access to the personal identification information being stored or being in transit between both SAPS and DoHA. According to the findings, all these measures are at not only complying with policy, but to also ensure that the privacy of citizens is not violated. The revelation from the findings indicate that DoHA employees are more concerned about the privacy of citizens while some of the police officials regard the privacy procedures as mandatory to be followed.

Where automated access to information takes place, it was found that both departments utilizes passwords and user profiles which act as security measures to only allow access in accordance with prescribed limitation to ensure that only authorized users can view only what was prescribed for them to see. When the departments subjected their users to the authorization procedures, this was found to have brought consistency in the maintenance of privacy requirements since the departments' process personal details of citizens.

The findings reveal that there are concerns being raised by DoHA that privacy of individuals could be compromised if security measures are not adequately

implemented. Where remote and automated access to information by SAPS, to information held by DoHA can be implemented without proper security measures, this can raise potential threats of hackers who can remotely access the system to violate the privacy of citizens or contaminate the information to distort evidence for instance, which might work against crime operations.

It was also found that maintenance of privacy was as high amongst the police as it was for DoHA, this was found to be due to the feedback from DoHA regarded as being direct related to crime. Violation of both security and privacy raises concerns of the police since this is associated with the contamination of evidence where crime levels may go up as criminals may fake their identities and impersonate others for instance, and commit more crime. Violation of privacy therefore is found to inhibit crime operations. By contrast, if the police can comply with the requirements of privacy as laid down by DoHA, it was found that this would enable crime operations since DoHA regards compliance to privacy as a condition to supporting access or automated access, by SAPS to information at DoHA.

SAPS and DoHA share the same security objectives since the former views unauthorized access to information impacting on validity of evidence while for DoHA, this constitute a persistent and serious crime of stolen identity that is causing the department countless problems. Since both departments are in agreement on the need to enhance crime reduction, and they are also in communication and agreement on the manual and automated security measures, the formulation of e-governance policy would be easier achieved to automate access by SAPS to information held by DoHA.

5.7.4 The analysis of crime reduction against global trends

In terms of this research, crime reduction operations are in relation to those carried out through the identification of perpetrators where the police can take appropriate actions like effecting arrests, charging or releasing perpetrators, for instance. Since the successful identification of perpetrators requires the cooperation

of more than one department, the integration of systems and information of the participating institutions has become necessary.

According to the literature review, Schiller says that that the police department, like the Erlanger, Ky., police department that used manual operations to process crime information faced numerous challenges and could not share information and benefit from the integrations. Once the department automated their systems and integrated with other operational areas and departments, the officers could quickly access information or share it across different operational areas to identify perpetrators even when driving in patrol cars. Crime intelligence, which concerns information that is manipulated to help the police prevent, combat and reduce crime, is comprised of information that is integrated from various sources that produce crime relevant information.

In order to reduce crime, the police have to collaborate with many different organizations. This was evidenced from the Nigerian authorities when they built their crime intelligence system to reduce crime. According to Alese and Falaki (2007) the Nigerians included various different government agencies and stakeholders' whose information requirements were taken into account to facilitate ease of access to its information by all who are concerned and authorized while it also enables inputs from various internal and external sources.

5.7.5 The analysis of policy formulation against global trends

Access to information policy promotes access by everyone, to information held by government as well as promoting for security to be implemented to protect the information against privacy violation for instance. The government undertook efforts at creating an environment of transparent and participatory policy formulation processes including information policy. The government also tried to comply with the freedom of expression and freedom of access to government information rights as enshrined in the Constitution ant took various initiatives on access to information that were also put in place to ensure the attainment of universal access to government information. The initiatives included the implementation of government to citizens'

communications through multi-purpose community centers (MPCC) and implemented a mechanism to survey the implemented MPCC to establish means of strengthening them to achieve their intended purposes.

According to Jaeger (2007) information policy provides the control measures which are necessary to put in place some limits or security to exclude access to certain types of information where privacy concerns may be sited as the reason for instance. Buckland (1991) says that in order to be as inclusive as possible and to reach as many communities as possible, the access to information policy makers must take various factors that enable access to information into account when formulating access to information policies. These can be in the form of communication language and the cost of the process of access to information for instance. By ensuring that a policy that enables access to information held by government is in place, this is ensuring compliance to international law (Mathiesen, 2008).

5.7.6 The analysis of legislation against global trends

The Promotion of Access to Information Amendment Act 54 of 2002. gives effect to the constitutional right of access to information held by government in a speedy, cost effective and effortless manner. According to the law, access to information held by government or any one has to be allowed if information is required for the exercise or protection of any rights. The law also gives effect to the right to privacy by everyone and thereby limiting the right of access to information under certain conditions.

According to Sharma and Gopal (2006) personal information in the hands of government is collected and used specifically for lawful functions and can be disclosed to third parties without the owner's consent strictly if it is permitted by law, if the disclosure thereof is for reasonably necessary for law enforcement *etc*.

While the legislation is in compliance with the global trends, it does not set out time frames or deadlines for the transfer of information to help SAPS to comply

with other legislation like the Criminal Procedure act which sets out the detention deadlines.

5.7.7 The analysis of e-governance findings between SAPS and DoHA

Even though the departments have each developed e-governance programs for their internal automated access to information for identification of perpetrators and citizens at SAPS and DoHA respectively, automated access between the departments is not implemented to automate access by SAPS, to information held by DoHA. According to the findings, two of the reasons were revealed.

The first barrier is the requirement by the courts that all printed material from DoHA must bear the signature of the DoHA DG to be acceptable as evidence in courts. This renders printed material that can be remotely obtained by SAPS from DoHA through the automated process to be unrecognized and useless as evidence at the courts.

The findings also revealed that the second barrier was caused by the designs of both departments' systems which are incompatible and would need huge investment to design and implement the interfaces to link the two systems. This was evidenced by the failure of the DoHA system to instantly identify perpetrator owners of the latent fingerprints taken from the scenes of crime by the police. The latter identification process is the main source of focus for SAPS.

5.7.8 e-Governance development process against global trends

The Presidential National Commission in the Information Society and Development Plan or ISAD Plan (PNC-ISAD, 2006) is the entity that was used to initiate the e-governance development plan in South Africa and must therefore represent the executive coordinator that is required. According to Klischewski (2011), this complies with one of the conditions required for the successful development of e-governance, the presence of an executive with adequate authority to oversee the process.

The second requirement for successful e-governance development process is an adaptive policy and regulations as explained by Paskaleva-Shapira (2006) which

Michel (2005) says should be continually evaluated. South Africa addressed this requirement when the IT policy framework and regulations were formulated to provide guidelines for all public institutions to implement various initiatives that are aimed at better government (DPSA, 2001).

Failure to comply with the e-governance development requirements results in the implemented solutions failing to deliver the desired benefits which Klischewski (2011) explains as the delivered of architectures that are not relevant to the specific context.

5.7.8.1 Automated access to information in South Africa

South Africa has set Minimum Inter-operability Standards (MIOS) which laid a foundation for effective government to government (G2G) communications that utilizes e-governance to automate access by a department to information held by another department. This process is regulated through the Amendment of Public Service Regulations of 5 January 2001 (RSA, 2001).

According to Shapard (1996) all government departments locally or globally are either in the process of inter-connecting to share information or have already implemented. e-Governance has the interoperability function that is capable to integrate the systems of the departments that are remotely dispersed while enabling the systems to be controlled by different individuals who may be locally or remotely located and yet achieving this feet at optimized and integrated government operations at lower operational costs (Klischewski, 2011).

Gordon (2002) says that e-governance can also be utilized to transform the traditional hierarchical organizational structures that operated separately in silos of authoritarian top down decision and policy making models to multiple departments or agencies that collaborates through loosely coupled networks. Joia (2004) refers to these traditional structures as outdated workflows within or between government departments and says that they can be replaced by establishing digital links.

e-Governance achieves this feet by performing the Horizontal integration to integrate departments within the same level or the Vertical integration for different

levels of government departments or tiers of government such as national, provincial and local OECD (2003a). The integrations enable the departments to operate as a single organization that adopts shared platforms for the core technologies on which to execute common applications.

The Enterprise Application Integration (EAI) is an example of an integrated e-governance model. There are four requirements for a successful implementation of e-governance integration model to share information between departments.

Fan and Zhang (2007) names the four requirements where the first one, the Environmental requirements refer to a central coordinating executive who has adequate authority over the participating departments to control and coordinate the integration process. The second condition is the Intra-organizational requirements which require the top organizational support for the integrations.

The third condition refers to the Inter-organizational requirements which require the need for the participants to have trust that the participants will all act in the best interest of the integrated environment. The fourth and last condition, the Perceived performance requirements refer to the perceived benefits of the integrated solution.

5.7.8.2 e-Governance security

The country has set the Minimum Information Security Standards (MISS) to control the security of information during automated access by a department to information held by another department. This process is regulated through the Amendment of Public Service Regulations of 5 January 2001 (RSA, 2001). MISS specifies security standards due to possible integrations of public operations and services (RSA, 2001). These standards define the requirements and conditions that are prerequisite for the security of a connected and web-enabled government.

e-Governance provides security measures such as the encryption technique that can protect information that is being shared between two or more departments. The technique renders information in the network and being illegally intercepted by hackers to be unreadable and useless to them since they are not in possession of a

decryption key like the Public Key Cryptosystem and Agency Identification for instance. The public Key is applied to decode the information back to readable format (Sharma and Gopal, 2006 and Headayetullah and Pradhan, 2009)

5.7.8.3 e-Governance policy process against global trends

The Department of Public Service and Administration (DPSA) as the custodian of the development of ICT plans implemented an ICT policy framework for government which is to provide guidelines for government ICT development. During policy formulation, broad consultation ranging from the presidency up to grass roots levels were undertaken and efforts implemented to ensure central coordinated ICT procurement to standardize the national ICT infrastructure and applications.

The DPSA policy framework contains various recommendations that include e-government initiatives that address the intra-governmental operations or G2G to address access by a department, to information held by another department. The policy also specifies the accessibility and security standards which are the Minimum Inter-operability Standards (MIOS) and the Minimum Information Security Standards (MISS) respectively.

e-Governance policy development can be achieved through consultations where the process can be done interactively with other government departments or stakeholders (Michel, 2005 and Paskaleva-Shapira, 2006). Michel further points out that policy can continually undergo evaluation process.

Various writers including Paskaleva-Shapira and Singh (2010) share the same view that the objectives of e-governance are the same as those for good governance. This means that e-governance policy has to address, amongst others, the accessibility and security requirements of information. The latter is necessary to protect sensitive or personal information to address concerns relating to privacy for instance. It has become important for e-governance policy to include the plans for acquisitions and implementations of the new technologies to ensure attainment of these requirements. Singh points out the importance of this as per the lessons learned from the Indian e-

governance development where it was discovered that ignoring the technical issues could render the implemented solutions not to comply with the policy requirements.

The e-governance' accessibility Policy should also specify and detail issues that must be taken into consideration for the quality of the integrated and shared information which can be maintained by the utilization of ICT public key infrastructure to maintain data integrity using MD5 algorithm (Headayetullah and Pradhan, 2009).

5.7.8.4 e-Governance security policy against global trends

The South African e-governance policy initiative for security calls for the security standards where the regulation sets up the Minimum Information Security Standards (MISS) for the security of information.

e-Governance security policy should provide for various security measures to protect and maintain confidentiality of information across the network between departments, for instance. Headayetullah and Pradhan (2009) suggest that the policy should include secure protocol that protects information for confidentiality by implementing ICT security applications like the Public Key Cryptosystem and Agency Identification using a unique mapping function.

5.8 Chapter summary and overview of next chapter

The policy guidelines that define the mandates of both SAPS and DoHA have been identified and taken into account during the analysis of the findings from both departments. The themes and findings have been analyzed and matched with operational practices by both departments.

The next chapter will provide the conclusions on practices by the departments as these will be compared against global trends and recommendation provided in the same chapter six.

CHAPTER SIX: CONCLUSIONS AND RECOMMENDATIONS

6.1 Introductions

This chapter provides the conclusions based on the analysis of the findings from the effects of policy on e-governance and recommendations. Policy plays a role on the success of crime reduction operations through its influence on e-governance which enables the automation of the identification of perpetrators of crime.

If our objective as a society is to reduce and prevent crime, then there are specific processes and knowledge that is required to make this a reality. The processes include means of automated citizen identification for all citizens in order to be able to effectively identify perpetrators of crime from amongst the total population.

Knowledge required to solve crime is about ICT skills required to perform automated and electronic access to information held by a department. However, it may not be sufficient simply to hold the electronic records of convicted criminals. It may be necessary to hold electronic records for all citizens and requiring citizens' records to be fully electronic and available. This raises policy concerns regarding citizens' rights to privacy versus government need for access to information to solve crime.

6.2 Conclusions

In order to attain the crime reduction objective of this research, the effects of policy on access to information held by government were studied. The aim was to reveal lessons needed for the formulation of effective e-governance policy to enable the automation of access to information held by government. The automation of access to information is necessary to enhance crime reduction through rapid identification of perpetrators.

The conclusions are based on the analysis of the findings. The findings revealed that while access to information policy was not adequately effective to enable automated access by SAPS, to information held by DoHA, there was another barrier in the form of the absence of a non-adaptive e-governance policy. Figure 6.1

is a schematic representation of policy enablers and barriers to automated access by SAPS, to information held by DoHA for the identification of perpetrators.

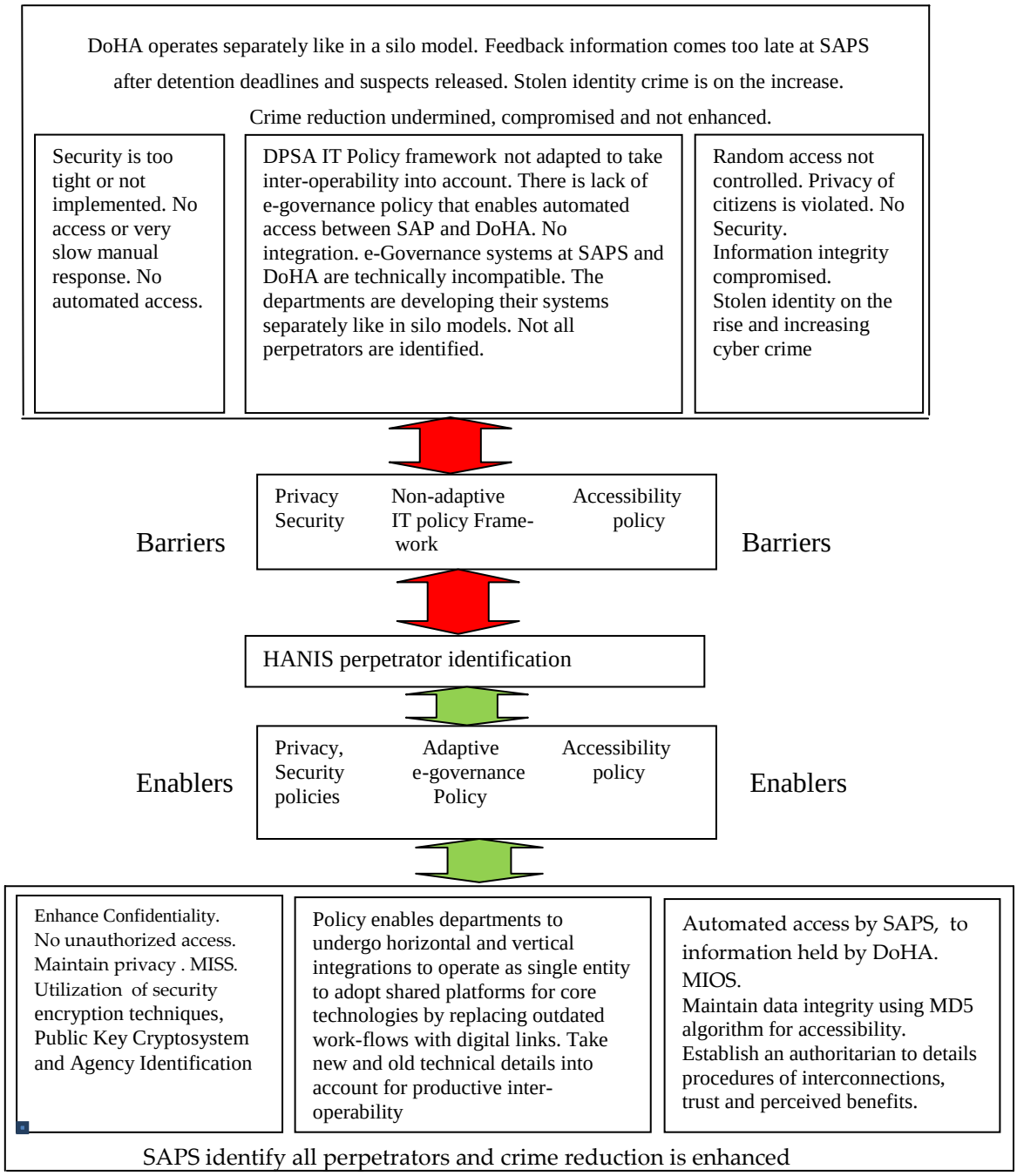
Figure 6.1 below indicates that while lack of policy constitutes a barrier to the development of e-governance, the reverse does not apply since its availability does not necessarily constitute an enabling environment. As the diagram shows, policy must not merely exist, but should be controlled and adapted to the changing environment that is mostly influenced by ICT. This is because policy may act as barrier or enabler. Even though there are other factors apart from policy that may play a role to affect access to information for the identification of citizens. Factors such as person's attitudes, levels of competencies with regards to the operations of the e-governance technologies and criminal elements amongst the persons within the departments revealed as playing minor roles in this study. The schematic representation is only based on the conclusions of the role played by policy on e-governance which is needed for the identification of perpetrators to enhance crime reduction.

6.2.1 Compliance with accessibility policy

The accessibility requirement of policy is about the promotion of access to information held by government. Policy calls for the right of access to information to be protected and effected. According to policy, access to information should only be used legally and for intended purposes since uncontrolled access to information my result in dangers of increasing stolen identity crimes for instance.

The Department of Home Affairs has fully complied with this requirement of policy in granting access by SAPS to information in its possession. The challenges and concerns that are raised about access to information being manually done, slow and not assisting the police in some cases, serve as indications of unintended outcomes of the current policy which is therefore not adequate to enhance crime reduction.

Figure 6.1: Schematic representation of policy role on crime operations



Source: *Motlhabane, G, 2011*

6.2.2 Compliance with the security policy

The security requirement of policy is about the promotion of the safety and protection of information held by government so that it is not used for unintended purposes.

The Department of Home Affairs has fully complied with this requirement of policy in granting controlled access by SAPS to protected information in its possession. Security measures for manual and automated access to information were found to be implemented by both departments in their areas. There are agreements between them about the security measures and how access to information will be controlled to ensure their adequacy not to be too tight or otherwise to stifle or allow uncontrolled access to information. Security measures for both manual and automated access to information are however time consuming during identification of the police at SAPS, access control at entrances and the authentication of application forms for information. These measures delays the feedback from DoHA needed for crime reduction and therefore act as barriers to access and automated access by SAPS, to information held by DoHA.

6.2.3 Compliance with the privacy policy

The requirement of privacy policy is about ensuring that information of private citizens held by government is not used without their permission except as permissible by law.

The Department of Home Affairs has fully complied with this requirement of policy in granting access by SAPS to reliable and non-contaminated information in its possession. In the case of automated access to information, this has also been carefully been granted through controlled password driven automated access by only authorized SAPS officials, to information in its possession. Both manual and automated security requirements involve processes such as continued identification of the police or being subjected to access control procedures to offices containing systems which act as barriers to crime operation due to delays.

6.2.4 The Identification of perpetrators against global trends

The crime reduction strategy of this research is about the utilization of e-governance for the identification of criminals.

Even though both SAPS and DoHA have implemented e-governance to automate their internal access to information for rapid identification of perpetrators and citizens respectively, e-governance is not implemented to integrate their systems to enable automated access by SAPS, to information held by DoHA. This is due to a lack of an effective e-governance policy. The current access to information policy does not provide for automated access, by a department to information held by government.

The Erlanger police department improved their identification process after they automated their systems and integrated with other departments and was able to quickly access information where they could identify perpetrators even when driving in patrol cars. The integration of the systems with other departments is a key requirement to the successful identification of all perpetrators. South Africa has therefore not complied with the global trends where SAPS and DoHA did not connect and integrate their systems.

6.2.5 The formulation of policy versus global trends

Even though access to information legislation in South Africa did not follow the normal policy formulation process that precede the law making, there has been various initiatives that were taken that include Freedom of Expression and Freedom of Access to Information process, Transparent information policy formulation process and Government policy initiatives on access to information which were undertaken at various stages towards formulating access to information policy.

These initiatives led to the conclusion that South Africa follows a consultative and transparent process of policy formulation. By consultations, South Africa caters for the global requirements of taking factors that affect access to information into account since various languages have been included as communication medium to be accommodative to various ethnic groups. The

country's policy also complies with the right of access to information in public office since this is also enshrined in the Constitution. This is in compliance with the explanations of Jaeger (2007) about how information policy controls access to information. The local privacy policy calls for security measures to be implemented for legal and authorized access to information in compliance to accommodating the privacy concerns of citizens which Singh (2010) says is for confidentiality of personal information. Even though South African policy formulation follows the internationally accepted trends, the information policy and various initiatives taken to enable access to government information, access by SAPS to information held by DoHA does not enhance crime reduction. This is because South Africa did not fully comply with global norms since even though policy formulation is based on consultations, there is no policy that governs access, by a department, to information held by another department. If this was the case, the departments would take into account other departments' needs and considerations when building their systems. The current policy therefore is inadequate and not adaptable to the current situation to enhance crime reduction.

6.2.6 The South African legal implementation against global trends

The access to information law gives effect to the right of access to information held by government while limiting the right under certain conditions such as for the protection of citizens' privacies. South Africa therefore complies with international trends since globally, personal information in the hands of government should be collected and used specifically for lawful functions and can be disclosed to third parties without the owner's consent strictly if it is permitted by law, if the disclosure thereof is for reasonably necessary for law enforcement.

Since the access to information legislation does not set out transaction completion deadlines, and seeing that the Criminal Procedure act does set out detention time limits or deadlines, this points to the laws being enacted in isolation without coordination with other relevant laws.

6.2.7 The impact of policy on e-governance between SAPS and DoHA

SAPS and DoHA may have implemented e-governance to automate access to information for the identification of perpetrators and citizens respectively but this does not enhance crime reduction since e-governance is not implemented to automated access by SAPS, to information held by DoHA. The reasons for this have nothing to do with the policy practices by DoHA officials as per the analysis of the findings. This has to do with the lack of an effective and adaptable e-governance policy that is necessary to guide e-governance development process of government. This problem has resulted in the design of the SAPS and DoHA systems being technically incompatible. While the accessibility requirement of policy in this regards has been fully complied with by DoHA, lack of adaptable e-governance policy has however been the reason that each department has developed their e-governance separately and did not take into account, other departments' needs of access to information.

6.2.8 e-Governance development versus global trends

The development process of e-governance in South Africa follows the path of global trends that require wider consultation and higher management involvement to control and coordinate the developmental operations. South Africa is fully in compliance with these conditions as the e-governance development process followed a wide consultative strategic approach that was initiated by the President through the PNC – ISAD plan. The country complies with the second global requirement of a guiding policy and regulation by formulating the IT policy framework document (DPSA, 2001) and an Amendment of Public Service Regulations of 5 January 2001 (RSA, 2001) respectively to guide the national e-governance development.

South Africa may have complied with the requirements to a certain extend however the IT policy and regulations are not continually evaluated since they are not adaptive to the specific departments' needs. Failure to comply fully with requirements leads to failure of the delivered solution to yield benefits (Klischewski, 2011). This has resulted in each department developing its e-governance systems

separately and led to technical incompatibilities between SAPS and DoHA. The failure of this approach is reflected by the lack of e-governance automation of access by SAPS, to information held by DoHA.

6.2.8.1 The effects of development on automated Access to information

South Africa implemented measures for automated access between departments such as the Minimum Inter-operability Standards (MIOS) and can possibly include quality standards for the integrated information as per global norms. According to Headayetullah and Pradhan (2009) ICT public key infrastructure can be utilized to maintain data integrity using MD5 algorithm.

Shapard (1996) says that all government departments locally or globally are either in the process of inter-connecting to share information or have already implemented. South Africa is still lacking in the government department systems inter-connections to share information. This means that the country or SAPS and DoHA have failed to utilize e-governance which, according to Gordon (2002) can transform the traditional hierarchical organizational structures which operate separately in silos of authoritarian top down decision and policy making models, into the departments that function as multiple departments that collaborates through loosely coupled networks and lower total costs.

The separate operations of SAPS and DoHA shows that South Africa has not developed and implemented e-governance to follow the global trends where e-governance can be utilized perform the horizontal and vertical integration of the departments that would enable them to operate as a single organization that adopts shared platforms for the core technologies on which to execute common applications OECD (2003a). The country does therefore not benefit from possible better government quality services at lower costs. Under these conditions, SAPS would be able to identify all perpetrators with less effort.

Even though South Africa is lacking behind the integration trends of e-governance for the automation of access by a department, to information held by

another department, the country is in compliant with the four conditions for the implementation of the automated data sharing model listed by Fan and Zhang (2007).

The first condition, the Environmental requirements refer to a central coordinating executive who has adequate authority over the participating departments to control and coordinate the integration process. The President fulfills this role through the PNC – ISAD plan (PNC – ISAD, 2001). The second condition is the Intra-organizational requirements which require the top organizational support for the integrations. DPSA has been appointed to control and coordinate as the custodian of the public ICT implementation strategy plans and can therefore represent this function to comply with the second requirement by coordinating and communicating at top management level to ensure organizational support.

The third condition refers to the Inter-organizational requirements which require the need for the participants to have trust that the participants will all act in the best interest of the integrated environment. South Africa achieves this at various levels starting at the PNC-ISAD Plan through the departmental top management representatives, the Government Information Technology Officers who hold occasional meetings that are chaired by their counterpart from the DPSA.

The fourth and last condition, the Perceived performance requirements refer to the perceived benefits of the integrated solution. This condition was complied with through the PNC-ISAD plan which includes the description of the Vision 2014 as the creation of the information society. According to this description, the information society utilizes ICT correctly to yield benefits in the form of modernized ICT infrastructure that enables government to offer top quality services that attain ICT universality while contributing positively to the socio-economic developments of South Africa.

Despite these compliances plans and structures, South Africa has failed to implement them when failing to enforce departments to follow the plans through and also failing to adapt the e-governance policy to identify various needs by certain departments. This has resulted in separate e-governance development by departments

and incompatible technical designs that inhibit automated access, by a department to information held by another department to the detriment of the safety of citizens.

6.2.8.2 The effects of development on e-governance security

South Africa is in line with global trends when it comes to the security measures that are set up for the possible protection of information in the network between departments. The measures are in the form of the MISS being set up for automated access to information between departments. This is in compliance with global security measures such as the encryption techniques which Headayetullah and Pradhan (2009) explains as the Public Key Cryptosystem and Agency Identification for local and remote automated access to information. According to the explanations, the techniques render the illegally intercepted information to be unreadable and useless to the hackers.

6.2.8.3 The effects of development on e-governance policy

The Department of Public Service and Administration (DPSA) as the custodian of the development of ICT process has implemented an ICT policy framework for government. DPSA further coordinates and engages in wide consultation with all the departments through the GITO council meetings. This is in accordance with how a successful e-governance policy formulation can be achieved as presented by Michel (2005) and Paskaleva-Shapira (2006). They are saying that the consultations can be enhanced through remote interactive communications between government departments.

South African e-governance policy complies with the accessibility and security of information requirements through the regulation of MIOS and MISS. In order to cater for global trends to control the procurement and standardize the ICT infrastructure across departments, DPSA created SITA to achieve this and comply with requirements to harmonize the old and new technology infrastructure and ensure that technical requirements are taken into account. The country however did not implement as planned to comply with the standardization requirement since the systems at SAPS and DoHA are technically incompatible to effect access by SAPS,

to information at DoHA. This is because e-governance policy was not adapted to consider the role certain departments could play in assisting others to achieve their mandates. DoHA has a specific role to pay for all other departments who seek to identify and verify the identities of citizens. An adaptable e-governance policy is therefore lacking in South Africa.

The quality of network information being catered for by MIOS can be adapted to include the utilization of ICT public key infrastructure which is emphasized by Headayetullah and Pradhan (2009) as necessary to maintain data integrity using MD5 algorithm.

6.2.8.4 The effects of development on e-governance security policy

The South African e-governance policy initiative for security calls for the security standards where the regulation sets up the Minimum Information Security Standards (MISS) for the security of information. e-Governance security policy should provide for various security measures to protect and maintain confidentiality of information across the network between departments, for instance. Headayetullah and Pradhan (2009) suggest that the policy should include secure protocol that protects information for confidentiality by implementing ICT security applications like the Public Key Cryptosystem and Agency Identification using a unique mapping function. South Africa should not have any problem in adapting if not yet done so since ICT products can be bought of the shelves.

6.3 Recommendations

The objective of this research is to promote crime reduction through the implementation of e-governance that is needed to automate access to information held by government which is required to enhance the identification of perpetrators of crimes. Since this raises policy concerns of citizens' privacy violation against government need for access to information to reduce crime, the situation calls for an effective e-governance policy to enable automated access to information while setting up security measures to cater for privacy concerns.

6.3.1 The accessibility policy

The accessibility policy should be adapted to specify shorter time periods of access by SAPS, to information held by DoHA which should be better managed for faster feedback to enable the police for timely identification of perpetrators even if the process is manual. Policy can specify feedback time limits like "feedback to be provided within twenty four hours of working court hours after being received**".** The requests for identification information at DoHA should be based on the seriousness and the urgency of the request and these could be classified and appropriate actions defined for each within the accessibility policy.

6.3.2 The security policy

Security should not be implemented up to a point where the process stifles and delays daily operations. While its implementation is very important for various reasons including privacy, the security measures should be monitored and care taken to ensure that the measures are not responsible for any delay that might jeopardize the crime reduction efforts. The security policy should include clauses that exempt the police from avoidable delaying checks during requests for access to information.

6.3.3 The privacy policy

The security measures that are implemented are done so to protect the personal information against privacy violation. The security system should therefore ensure that only authorized access to information takes place within time limits that are specified. Identification levels could be categorized and less sensitive information like just confirmation of owner of finger prints could be remotely provided by DoHA. SAPS could remotely submit, for instance, ID. number and name and receive a remote response that say "Match" or "No Match" where after a higher level verifications can take place for an appropriate action like effecting an arrest for instance, could be effected.

6.3.4 Crime reduction recommendations

Since crime reduction operations in this research are based on the identification of perpetrators, and the process can be enhanced by e-governance,

South Africa should follow that example of the rest of the world where governments have either connected or are in the process of connecting their departments to share information. This could be based on the example of The Erlanger, Ky., police department which improved their identification process after they automated their systems and integrated with other departments and were able to quickly access information where they could identify perpetrators even when driving in patrol cars.

6.3.5 Information policy formulation

Even though the South African policy formulation process follows the global trends of wider consultations and take factors that influence access to information into account to ensure that all stakeholders' views and interests are accommodated, policy should be adapted to regulate departments like DoHA differently. The differences in the public institutions and in how they can provide certain services to other public institutions must be taken into account by policy. As the national hub of the identification information where all other departments are dependent on it for the identification, authentication of identity documents as well as verification for positive identification of citizens, DoHA should be regulated to identify this important role that the department plays in the effectiveness of the operations of other departments. This makes DoHA a special and unique department that can offer essential services to other departments

Access to information policy should have specific provisions that regulate DoHA differently where policy takes into account its essential services to other departments. These provisions should be created outside DoHA at DPSA and the GITO council be allowed to play a major role so that the policies and regulations that emerge, would cater for the rest of the departments and be adaptive for emergency identification requirements, for instance, to promote and maximize national interest.

The stakeholder consultation of DoHA or information policy formulation must not only be about how the project is going to benefit it, but should be about how other departments are going to benefit. This calls for DPSA to centrally coordinate this process while all other departments must not develop their e-

governance project until they know how DoHA is going to develop its database and how are other departments who are offering essential services elsewhere and who may require access to information held by DoHA are going to access it. Access by SAPS, to information held by DoHA should for instance, where possible, be based on the needs of crime reduction operations while being adaptable to other departments.

6.3.6 The formulation of legislation

Since the detention deadlines set out in the Criminal Procedure act undermines the crime reduction efforts of the police who are utilizing the Promotion of Access to Information act for the identification of perpetrators, it would be beneficial to crime reduction if the enactment of laws were coordinated to take into account other relevant pieces of legislation. This access to information law would, for instance include shorter access to information deadline periods for the police at DoHA.

6.3.7 e-Governance development process

While global e-governance' best practices and trends serve as important guidelines that are formulated by experts who are exposed to latest state of the art or sophisticated and innovative practices and ICT advancements, every situation has its unique requirements that may mostly not be catered for by the global experts. The global e-governance development guidelines should be used as general guiding criteria but the detailed unique and local challenges must be analyzed more closely and global trends must be adapted and customized to specific local challenges to maximize local output.

e-Governance development process in South Africa is mostly based on best global practices even though the process is lacking in some cases. The IT policy framework that was established by the DPSA should continually be evaluated to be adaptive to the dynamic nature of the requirements of e-governance. This should be adapted to ensure that the departments develop and implement their e-governance systems together where the GITO council to ensure that there is a technical

standardization across the departments to achieve technical compatibilities between departments' systems where automated access by SAPS, to information held by DoHA could be enabled.

DoHA employees have revealed that massive investments would be required to adapt the system for automated access to its information by SAPS. Where DoHA is allowed to develop its e-governance systems, the interface costs can be avoided in future where all other public institutions must be made aware of how identity numbers for instance are going to be stored or retrieved by waiting for DoHA to develop and complete its e-governance projects or DoHA has make the design documents available to all these departments. This would avoid the need to build expensive interface applications trying to link the systems after they have already been completed.

A new e-governance policy that recognizes this important feature of DoHA and others that may be in the same situation has to be formulated to take control of e-governance development process out of the jurisdiction of DoHA and shift this to a central coordinating authority that has the national responsibility and accountability such as DPSA in liaison with the GITO council or any similar structure. This could be to the benefit of the entire nation.

6.3.7.1 Automated Access to information

Since all other government departments locally or globally are either in the process of inter-connecting to share information or have already implemented, South Africa should follow suite to enable automated access by SAPS, to information held by DoHA. By this interconnection, South Africa should be able to transform the traditional hierarchical organizational structures or departments that operate separately in silos into the departments that function as multiple departments that collaborates through loosely coupled networks.

The country should follow global trends where e-governance is utilized to perform the horizontal and vertical integration of the departments that would enable the entire government departments to operate as a single organization that adopts

shared platforms for the core technologies on which to execute common applications and eliminate duplication costs while improving on services. South Africa would not experience any difficulty for this transformation since the country is in compliant with the four conditions for the implementation of the automated data sharing model. Once achieved, the transformed environment would enable automated access by SAPS, to information held by DoHA.

6.3.7.2 e-Governance security process

The recommendations for the current e-governance security measures, the MISS can be upgraded to or combined with the encryption techniques such as the Public Key Cryptosystem and Agency Identification for local and remote automated access to information. The techniques would provide the security measures to protect the citizens' privacies by rendering the illegally intercepted information to be unreadable and useless to the unauthorized hackers.

6.3.7.3 e-Governance policy process

DPSA should continually evaluate and adapt the ICT policy framework for government. DPSA should further maintain the coordination of the evaluated process that include a wide consultation with all the departments through the GITO council and other relevant structures to ensure that there is always an existing e-governance policy that is current and relevant to the e-governance needs of the country. The consultation should help the DPSA to maintain an e-governance policy that achieves the standardization across the departments. Such a policy would also enable automated access by SAPS, to information held by DoHA.

The e-governance policy should also cater for the quality of the network information by setting the currently utilized Minimum Information Inter-operability Standards (MIOS) to include the specifications for ICT public key infrastructure that is necessary to maintain data integrity using MD5 algorithms.

6.3.7.4 e-Governance security policy formulation

The South African e-governance security policy should set up the currently utilized Minimum Information Security Standards (MISS) to accommodate the

secured protocol that protects information for confidentiality by implementing ICT security applications like the Public Key Cryptosystem and Agency Identification using a unique mapping functions.

REFERENCES

Adeola, S., Alese, B., & Falaki, S. (2007). The national crime operations system. *Information Technology Journal 6(*5*),* 633-647. Retrieved from EBSCO HOST database.

Babbie, E. (2004). *The practice of social research.* (10th ed.). Belmont, CA: Wadsworth.

Barth, N. (2011). Access to information: Assessment of the use of automated interaction technologies in call centers. *RAE, 51*(1), 27-42.

Batista, C. (2003). UNESCO. *ICTs and good governance*: *The contribution of information and communication technologies to local governance in Latin America*. Brazil. Retrieved on 17 August 2010 at: http://portal.unesco.org/ci/en/files/11316/10547335250Report_on_e-governance_in_Latin_America.pdf/Report%2Bon%2Be-governance%2Bin%2BLatin%2BAmerica.pdf

Bell, J. (2005). *Doing your research project,* Maidenhead: Open University Press.

Buckland, M. (1991). Information and Information Systems. Westport, CT: Greenwood Press.

Bush, T. (2007). Authenticity in research – reliability, validity and triangulation. In A. R. J. Briggs & M. Coleman (Eds.), *Research methods in educational leadership and management* (pp. 91–105), London: Sage publications.

Council of Europe, (1950). *Convention for the protection of human rights and the Fundamental Freedoms.* Rome. Retrieved on 08 August 2010 at: http://conventions.coe.int/Treaty/EN/Treaties/html/005.htm.

Council of Europe, (1981). *Convention for the protection of individuals with regard to automatic processing of personal data*. Strasbourg. Retrieved on 13 August 2010 at: http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm.

Creswell, W. (2002). *Research design*: *Qualitative, quantitative and mixed methods approach.* (2nd ed.). Thousand Oaks, CA: Sage publications.

de Lint, W., O'Connor, D., & Cotter, R. (2007). Controlling the flow: Security, exclusivity, and criminal intelligence in Ontario. *International Journal of the Sociology of Law, 35*(1), 41-58. Retrieved from Sciencedirect database.

DoHA (no date). Department of Home Affairs website. Retrieved on 14 June 2011 from http://www.home-affairs.gov.za/.

DPSA, (2001). Department of Public Service and Administration. (2001, February). *Electronic government, The digital future*. *A public service IT policy framework.* Pretoria. Retrieved on 4 September 2010 at: www.dpsa.gov.za/documents/acts&regulations/frameworks/IT.pdf

European Union, (1995). Directive 95/46/EC: *European parliament and of the council of the protection of individuals with regard to the processing of personal data and on the free movement of such data*. Strasbourg. Retrieved on 20 July 2010 at: http://*eur*-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

Fan, J., & Zhang, P. (2007). A Conceptual model for G2G information sharing in e-government. Retrieved at: http://it.swufe.edu.cn/UploadFile/other/xsjl/sixwuhan/Paper/EB372.pdf

Fang, Z. (2002). e-Government in digital era: Concept, practice, and development. *International Journal of the Computer, the Internet and Management, 10*(2), 1-22.

Farelo, M., & Morris, C. (2006). The status of e-government in South Africa. Retrieved from: http://researchspace.csir.co.za/dspace/bitstream/10204/966/1/Farelo_2006_D.pdf

Finger, M., & Pécoud, G. (2003). From e-government to e-governance? Towards a model of e-governance. *3rd European Conference on e-Government*. Trinity College Duplin: Ireland. Retrieved at: http://www.idt.unisg.ch/org/idt/ceegov.nsf/e73a24117ec5b5b6c1256d2c0054de28/22d6fea675a00d58c1256ddb002e3d89/$FILE/egovernance.pdf

HANIS, (no date). NEC, AFIS for identity management website. Retrieved from: http://www.nec.com/global/cases/sa/pdf/catalogue.pdf.

Henderson, S. C., & Snyder, C. A. (1999). Personal information privacy. Implications for MIS managers. *Information & Management, 36*(4), 213-220.

Headayetullah, M. D., & Pradhan, G. K. (2009). A novel trust-based information sharing protocol for secure communication between government agencies. *European Journal of Scientific Research 34*(3), 442-454. Retrieved from: //www.eurojournals.com/ejsr.htm.

Interpol, (2011). Criminal intelligence analysis. Retrieved on 23 July 2011 at: http://www.interpol.int/Public/cia/default.asp.

ITWeb, (2007, in press). South African Police Services. *MorphoTouch still the scourge of criminals*, Percy Morokane, South African Police Services Captain, by Leon Engelbrecht 16 January 2007. Retrieved at: http://ww2.itweb.co.za/sections/computing/2007/0701161400.asp?A=COM&S=Computing&T=News&O=C

Jaeger, P. (2007). Information policy, information access, and democratic participation: The national and international implications of the Bush administration's information politics. *Government Information Quarterly. 24*(4), 840-859. Retrieved from Sciencedirect database.

Joia, L. (2004). Developing government-to-government enterprises in Brazil: A heuristic model drawn from multiple case studies. *International Journal of Information Management, 24*(2), 147-166. Retrieved from Sciencedirect database.

Khoumbati, K., & Themistocleous, M. (2006). Integrating the IT infrastructures in healthcare organizations: A proposition of influential factors. *The Electronic Journal of e-Government, 4*(1), 27 – 36. Retrieved from EJEG database.

Klischewski, R. (2011). Architecture for tinkering? Contextual strategies towards interoperability in e-government. *Journal of Theoretical and Applied Electronic Commerce Research, 6*(1), 26-43.

Lor, P. J., & Van AS, A. (2002). Work in progress: Developing policies for access to government information in the New South Africa. *Government Information Quarterly 19*, 101-121. Retrieved from Sciencedirect database.

Luna-Reyes, L. F., Gil-Garcia, J. R., & Cruz, C. B. (2007). Collaborative digital government in Mexico: Some lessons from federal web-based inter-organizational information integration initiatives. *Government Information Quarterly, 24*(4), 808-826. Retrieved from Sciencedirect database.

Mack, N., Woodsong. C., MacQueen, K., Guest, G., & Namey, E. (2005). Qualitative research methods: A data collector's field guide. *Family Health International.* Retrieved at: Http//www.fhi.org.

Mathiesen, K. (2008). University of Arizona. *Access to Information as a Human Right*. Retrieved at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1264666

McMillan, H., & Schumacher, S. (2006). *Research in education*: *Evidence-based inquiry*. (6th ed.). Boston: Pearson education.

Michel, H. (2005). e-Administration, e-government, e-governance and the learning city: A typology of citizenship management using ICTs. *The Electronic Journal of e-Government, 3*(4), 213-218. Retrieved from EJEG database.

Mills, E. (2003). *Action research. A guide for the teacher research*. (2nd ed.). New Jersey: Merrill Prentice Hall.

Neuman, L. (2003). *Social research methods*: *Qualitative and quantitative approaches.* (6th ed.). Boston: Allyn and Bacon.

OECD, (1980). Organization of Economic Cooperation and Development. *Guidelines on the protection of privacy and trans-border flows of personal data*. Retrieved on 08 July 2010 at: http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html.

OECD. (2003). Organization of Economic Cooperation and Development. *e-Government imperative*: *OECD e-government studies*. Retrieved on 17 July 2010 at: http://www.oecdbookshop.org/oecd/display.asp?K=5LMQCR2K3HBP&DS=The-e-Government-Imperative

OECD, (2003a). Organization of Economic Cooperation and Development. *The Annual Report*. Retrieved on 11 August 2011 at: http://www.oecd.org/dataoecd/45/28/2506789.pdf

OECD, (2003a, p. 58). Organization of Economic Cooperation and Development. *The Annual Report*. Retrieved on 11 August 2011 at: http://www.oecd.org/dataoecd/45/28/2506789.pdf

Paskaleva-Shapira, K. (2006). Transitioning from e-government to e-governance in the knowledge society: The role of the framework for enabling the process in the European Union's countries. *Proceedings of the 2006 International Conference on Digital Government Research. 151*, 181-190.

PNC on ISAD, (2006). Presidential National Commission on the Information Society and Development. *Towards an inclusive information society in South Africa.* The PNC on ISAD, Pretoria.

Ratcliffe, J. (2007). Integrated intelligence and crime analysis: Enhanced information management for law enforcement leaders, office of the community oriented policing services, U.S. Department of Justice. (2nd ed.). Retrieved from: http://www.policefoundation.org/docslibrary.html and http://www.cops.usdoj.gov/

Republic of South Africa. (1996, December 16). *Constitution of the Republic of South Africa No. 108 of 1996*. Cape Town. (Government Gazette, Vol. 378, No. 17678).

Republic of South Africa. (1997, December 3). *Identification Act No. 68 of 1997.* Cape Town. (Government Gazette, Vol. 390, No. 18485).

Republic of South Africa. (1997, December 10). *Criminal Procedure Second Amendment Act No 85 of 1997*. Cape Town. (Government Gazette, Vol. 390, No. 18501).

Republic of South Africa. (2000, February 2). *The Promotion of Access to Information Act 2 of 2000*. Cape Town. (Government Gazette, Vol. 416, No. 31857).

Republic of South Africa. (2001, January 5) *Amendment of Public Service Regulations*. (Government Notice No. R. 1).

Republic of South Africa. (2002, February 2). *The Promotion of Access to Information Amendment Act 54 of 2002*. Cape Town. (Government Gazette, Vol. 451, No. 24250).

Republic of South Africa. (2003, December 22). *Criminal Procedure Amendment Act No 42 of 2003*. Cape Town. (Government Gazette, Vol. 462, No. 25862).

Republic of South Africa. (2008, August 14) *The South African Police Service Amendment Act No 57 of 2008.* Cape Town. (Government Gazette, Vol. 253, No. 25862).

Republic of South Africa. (2009, August 14). *Protection of Personal Information Bill*. (Government Gazette, number 32495).

Roberts, A. (2003). Access to government information: An overview of issues. Public Management Electronic Journal, (2). Retrieved at: http://e-journal.spa.msu.ru/images/File/2003/roberts(1).pdf

SAPS, (2010). The South African Police Services. *2009/2010 crime report.* Pretoria Retrieved at: http://www.saps.gov.za/statistics/reports/crimestats/2010/crime_situation_sa.pdf

Saxena, A. (Dr) (2004). Right to Information and Freedom of Press. New Delhi: Kanishka Publishers Duistributers.

Schiller, K. (2011). Information builders: Fighting crime with analytics. *Information Today, 28*(1), 37-37.

Shapard, R. (1996). Information superhiways: Cities and counties get plugged in. *The American City & County*, *111*(2), 20-24.

Sharma, S. and Gopal, K. (2006). Right to information: Implementing information regime. Jawahar Park Laxami Nagar, Delhi: Authorspress Global Networking.

Singh, A. (2010). Role of information technology in enabling e-governance. *I.U.P. Journal of System Management, 8*(1), 7-14.

Silverman, D. (2004). Qualitative research, theory, methods and practice. (2nd ed.). London: Sage publications.

Tellis, W. (1997). Introduction to case study. *The Qualitative Report, 3*(2). Retrieved at: http://www.nova.edu/ssss/QR/QR3-2/tellis1.html

Universal Declarations, (1948). United Nations. *Universal declarations of human rights of 1948, article 12*. Paris. Retrieved on 06 June 2010 at: http://www.un.org/en/documents/udhr/index.shtml

World Bank, (no date). World Bank. *Definition of e-government*: *e-Government*. Retrieved at: http://web.worldbank.org/

Xiao, H., & Smith, S. (2006). Case studies in tourism research: A state-of-the-art analysis. *Tourism Management, 27*(5), 738-749.

Yin, R. (1994). Discovering the future of the case study methods in evaluation research. *Evaluation Practice, 15*(3), 283-290. Retrieved from Sciencedirect database.

Yin, R. (2003). *Case study research*: *Design and methods.* (3rd ed.). Thousand oaks, CA: Sage Publications.

Yin, R. (2009). Case study research: Design and methods. *Australian Emergency Nursing Journal, 12*(2), 59-60. Retrieved from Sciencedirect database.

APPENDICES

Appendix 1: Interview Questions

Introduction

This Masters-level research explores the needs for greater efficiency and effectiveness in access to information, in order to benefit those working in crime reduction. It gathers data on the value of automated access to information, using information and communication technologies. The research aims to understand the challenges associated with rapid manual access to information and automated access to information. George Motlhabane is a post-graduate student completing a Masters degree at the University of the Witwatersrand.

Confidentiality

While all Masters research reports are available through the University Library, confidentiality will be observed with respect to the parties interviewed. The student does not require any information on crime reduction practices, which should not be made public.

Thank you for your participation.

Job Title/Rank	Department	City	Date	Time

1. Requirements of access to information policy.

1.1 How do the Officials comply with the policy requirements for accessibility, security and privacy?

1.2 What are the relevant procedures for meeting these policy requirements?

1.3 What are the concerns or challenges?

Accessibility		Security	Privacy
1.1			
1.2			
1.3			

2. Requirements of e-governance policy

2.1 How do the Officials comply with the policy requirements for accessibility, security, privacy?

2.2 What are the relevant procedures?

2.3 What are the concerns or challenges?

Accessibility		Security	Privacy
2.1			
2.2			
2.3			

3. Relevance of policy issues to crime reduction.

3.1 How do the accessibility, security and privacy requirements of information held by DoHA contribute to effective crime reduction?

3.2 How can these requirements inhibit or compromise crime reduction?

Accessibility		Security	Privacy
3.1			
3.2			

4. What is the extent to which manual access to information held in DoHA is a barrier or enabler to effective crime reduction within SAPS?

	Barrier	Enabler
4.1		

5. **What is the extent to which automated access to information held in DoHA is a barrier or enabler to effective crime reduction within SAPS.**

	Barrier	Enabler
5.1		

6. **How can policy requirement for privacy (manual access versus automated access) act as barrier to access to information held by DoHA?**

Privacy		
	Manual Access	Automated Access
6.1		

7. **How can policy requirement for security (manual access versus automated access) act as barrier to access to effective crime reduction?**

Security		
	Manual Access	Automated Access
7.1		

8. **How can the concerns associated with the policy requirement for privacy be addressed to present an enabling environment for effective crime reduction?**

Privacy		
Manual Access		**Automated Access**
8.1		

9. **How can the concerns associated with the policy requirement for security be addressed to present an enabling environment for effective crime reduction?**

Security		
Manual Access		**Automated Access**
9.1		

10. **How can the concerns associated with any policy requirement be addressed to present an enabling environment for effective crime reduction?**

Security		
Manual Access		**Automated Access**
10.1		

End of questions

Appendix 2: Letter of interview approval

Faculty of Commerce, Law and Management
University of the Witwatersrand,
Johannesburg
PO Box 601
Wits 2050

Tel: 27-11-717-3652
Mobile : 082 569 7675
e-mail:luciennesa@gmail.com(mobile email) and
lucienne.abrahams@wits.ac.za

25 January 2011

To Whom It May Concern

Dear Sir/Madam

LETTER OF REQUEST: RESEARCH STUDIES MASTER OF MANAGEMENT (ICT POLICY AND REGULATION)

Mr George Motlhabane, Student Number 0612110R, is a student on the Masters of Management (ICT Policy and Regulation) degree programme. He is currently completing his research on the topic "Automated access to information for crime reduction". Mr. Motlhabane needs to conduct between 12 and 18 interviews in order to collect data for this research report, which constitutes 50% of the credits towards the degree.

It would be sincerely appreciated if you would assist by granting him an interview to respond to the limited set of questions raised. It would also be very useful if there were any documents pertaining to the subject matter of the research that you could share with him.

We understand that there may be certain aspects of the topic which cannot be discussed for reasons of state security, however, the focus of the subject here is on the transition from manual to automated systems for managing and sharing information between two government departments. This falls within the broader frame of research interest, with respect to changes in government occurring based on the introduction of computing and the Internet, otherwise referred to as electronic government.

This is a very interesting subject and student research will enable us to have graduates who can further contribute to these developments in government and the private sector.

Should you require any further information, please contact the writer at 082 569 7675.

Yours sincerely,

Luci Abrahams, Degree Convenor: Masters of Management (ICT Policy and Regulation)
& Director LINK Centre, University of the Witwatersrand