Biometrics Application in Airport Security and the Individual's Right to Privacy

By

Ganeshwar Kumar Bhunjun

***

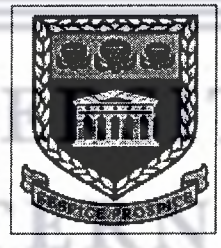
A thesis submitted in fulfilment of the requirements for the Degree of

Magister Commercii (Information Management)

in the department of Information Systems

at the

University of the Western Cape



Supervisor: Dr Glen Martin Mansfield

Co-supervisor: Yvette Goussard

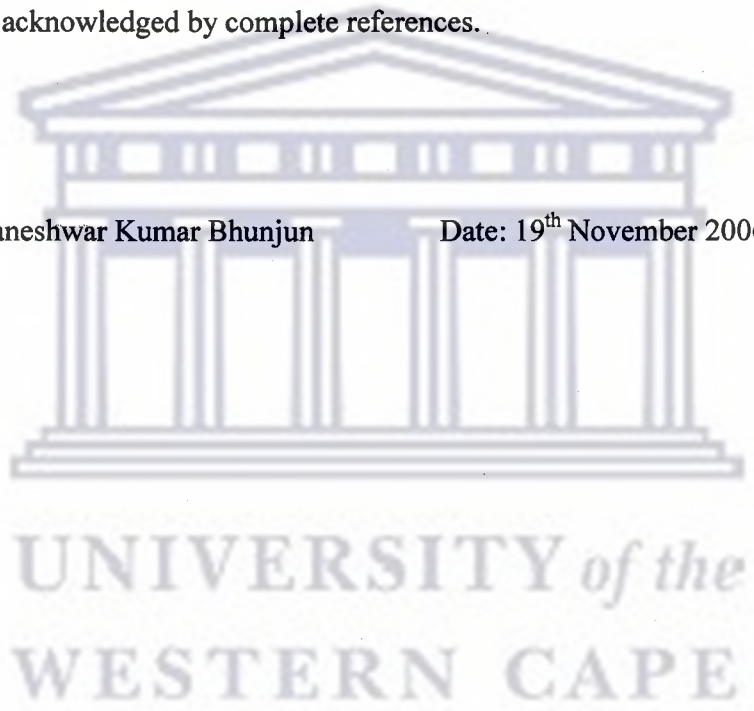
Wednesday, 21 February 2007

DECLARATION

I declare that *Biometrics Application in Airport Security and the Individual's Right to Privacy* is my own work, that it has not been submitted for any degree or examination in any other university, and that all the sources I have used or quoted have been indicated and acknowledged by complete references.

Full name: Ganeshwar Kumar Bhunjun Date: 19th November 2006

Signed:



ABSTRACT

Biometrics is the science of identification or verification of any individual based on that person's unique physiological and behavioural characteristics. As the application of biometrics technologies achieve global penetration, particularly in airport security, so individual privacy becomes compromised. This research examines the relationship between privacy and security, using South African air travellers as its focus, and airports as the specific area of application.

Two different approaches have been used for this research. The first is a literature-based approach that discusses the use of biometrics technologies and privacy concerns for airport security. The second method is empirical fieldwork in which questionnaires were used to measure the response of South Africans, residing in Cape Town, regarding their attitude towards the use of biometrics for authentication and their perceptions of the relationship between privacy and security.

This thesis tries to give an answer to the following questions:

- Will travellers accept biometrics for higher security measures, that is, positive authentication?
- Will passengers be willing to opt for higher security measures by giving up privacy?
- Are passengers prepared to make privacy sacrifices for the sake of convenience?

The response rate to the questionnaire was 91.3% from a sampling frame of 150. It delivered 136 usable responses. The survey findings indicate that all passengers

making international trips are familiar with fingerprint technology, as they have had to provide fingerprints for passport and/or driver's licenses. The opinion survey confirmed that South African passengers are more concerned about their personal security than privacy. Respondents would sacrifice privacy for higher security and convenience. The results also illustrate that the majority of individuals would accept using biometric technologies at the airport as a means to improved security.

Findings from this research make a contribution towards understanding public attitudes regarding the application of biometric technologies and individual privacy rights, specifically focused on the application at airport security.

ETHICS STATEMENT

The fieldwork of this study followed the University of the Western Cape guidelines on research ethics. The project involved people as research subjects. The researcher was fully aware of the necessary ethical considerations. All fieldwork was conducted in accordance with these guidelines. Specifically, for this research, the ethical considerations included ensuring that the researcher had the appropriate training and preparation for the work; the rights and welfare of the human subjects were protected; the identities and interests of those involved have not been disclosed; the information imparted has been anonymised and treated confidentially; and, the research was conducted in accordance with the ethical and professional practices of the information technology industry.

KEYWORDS

Biometrics

Informational privacy

Airport security

Authentication

Identification

Verification

Information practice

Integrity

Individual right to privacy

South African airports

ACKNOWLEDGEMENTS

First and foremost, I would like to show my gratitude to my supervisor **DR GLEN MARTIN MANSFIELD**. I am deeply indebted to him for his assistance, and encouragement for helping me to complete this research.

Secondly, I would like to thank my co-supervisor **MISS YVETTE GOUSSARD** for her passion for research and for proofreading my thesis. I owe her lots of gratitude for showing me the way of research journey.

I would also like to gratefully acknowledge the support of very special individuals. These are my uncles and aunties who helped me immensely by giving me encouragement:
Suresh & Anjani Ramsawhook,
Anand & Ragini Ramsawhook,
Vinod & Nandini Ramsawhook, and
Rajesh & Aarti Ramsawhook.

Especially for always believing in me and for their support, love, and appreciation, I would like to give my special thanks to my family:
Dad Jay Kumar Bhunjun, Mum Jaywuntee Bhunjun;
Uncle Jay Prakash Bhunjun, Aunty Sacheeta Bhunjun;
Grand father Manilall Bhunjun, Grand mother Dewantee Bhunjun;
Brothers Sailesh (Vodeshwar) and Krishna (Lekhanand), and
Cousins Pravesh (Kewatraj), Manoj and Shalini

Furthermore, to those who introduced me to the field of information system and who have had a remarkable influence on me during my six years at The University of the Western Cape, I wish to express my warm and sincere thanks to:
Professor Andy Bytheway,
Dr Kobus Smit,
Mr Grant Hearn,
Mr Thando Mjebeza, Mrs Marcelle Lodewyk, and Mr Cedrick Muleya.
And, also not forgetting **Professor Louis Fourie** and **Mrs Bongazana Mahlangu** for their support.

In addition, grateful thanks to **Mr Zakariya Mohammed** and **Mohammed B Elmalik** who became involved with this thesis by converting numbers into words, and to **Dr Hashim Issa Mohamed** for his help and suggestions for developing the questionnaire for the survey. Moreover, I dearly extend my thanks to each of the 137 anonymous respondents who took the time to complete the questionnaire.

And finally, to God for granting me the strength, patience and guiding me in the right path.

TABLE OF CONTENTS

LIST OF TABLES

LISTS OF FIGURES

LISTS OF APPENDICES

CHAPTER 1: INTRODUCTION

1. Introduction and Methodologies

1.1.Introduction and Outline of the Thesis

This chapter presents a summary of the study and gives an overview of the research context. The main research problem and the research questions are stated next. Then, an indication of the research framework is given and the research design is discussed. The research methodology follows.

1.2.Research context

The September 11, 2001, terrorist attacks on the Twin Towers and the Pentagon were devastating. Hijacked commercial airliners were sent crashing into the three buildings which resulted in the collapse of the Twin Towers causing the deaths of many thousands of people. Thousands more were affected by the loss of loved ones in the attack. People around the world were shocked and deeply concerned. This tragic event will forever be engraved in the minds of all people.

Such terrorist attacks are of major concern to all countries around the world. South Africa is no exception, especially when taking into consideration that the 2010 Soccer World Cup will be held here. The arrival of visitors from all over the world to South Africa will cause an influx of travellers at national and international airports. Therefore, the safety and security of every citizen and fan visiting South Africa for the world's largest sporting event, is a major factor of concern. The country's reputation will be at risk if, prior to the sporting event, something like the terrorist attack takes place here. State-of-the-art technologies however may be

applied to track and stop criminals. One such technology is biometrics. Biometrics, as explained later, is the automatic authentication of an individual.

The topic for this research was selected after reading articles related to the use of biometrics in enhancing security at airports. Many academic articles show that biometric techniques are being applied at airports in the United States and other European countries, such as Germany. Biometrics in itself is a very broad topic and is currently used in the business application domain and government programmes. The technologies are successful at some airports and ineffective at others. Biometrics could provide an option for strengthening the border security at the airports in South Africa.

Further reading of the literature provided increasing clarification for this research problem. The literature review gave an indication that although the benefits associated with the technology are numerous, one major concern is the individual's constitutional right to privacy. Proponents believe that such technology may actually be privacy-enhancing; its opponents, however, are against its use. Before implementing such a technology it is important to test the perception of South Africans regarding biometrics and its application.

A further reason for choosing this topic was due to the fact that no studies appear to have been done with regards to the use of biometrics in the border security at airports in South Africa. Therefore there is a need to explore, in depth, how South Africans' perceptions of biometrics are related to individual rights to privacy.

1.3.Title of research

The title of the topic is: ***"Biometrics Application in Airport Security and the Individual's Right to Privacy."***

Security of computers, buildings, Information Technology (IT) systems and other facilities have always been very important in order to protect organisations' sensitive data, individuals and/or their personal information. Airport security is one of the major areas that requires a high level of security as this industry is expanding rapidly. Millions of people are travelling around the world. Traditional authentication methods such as passports, passwords, personal identification numbers (PIN codes) are being used in order to identify the identity of individuals or travellers. Due to an increase in the sophistication of hackers, terrorists, and malicious third parties, however, there is a need to move towards more advanced technologies. One technology that has been identified to overcome such problems is biometrics, the automatic authentication of an individual, based on his or her physical characteristics. However, biometrics is not a universal panacea, and one of the problems identified related to biometrics is the impact upon the individuals' right to privacy. Privacy is the condition of an individual being left alone to determine for him- or her-self when, how and to what extent personal information may be transmitted to others (Udo, 2001).

1.4.Aims of the research

The aim of this research is to investigate the privacy concerns that individuals have regarding the use of biometrics for recognition at airports and understanding whether the security benefits associated with biometrics technologies outweigh privacy concerns.

1.5.Rationale for the study

1.5.1. Background to the problem

Biometrics is the automatic authentication of an individual based on his or her physiological or behavioural characteristics. Physiological characteristics refer to fingerprint, iris, retina, and hand geometry, whereas behavioural characteristics are involved with signature verification.

The use of biometric technologies in airport security is growing rapidly. After the September 11 terrorist attacks, most airport managers began to employ biometric technologies to authenticate an individual's physiological characteristics such as fingerprint, hand or palm geometry, iris scan, and facial recognition. As the cost of biometric technologies decreases, and their use spreads to other applications, privacy concerns associated with the technologies are raised. Travellers or customers need to be aware of how their personal or sensitive information is being used or processed.

1.6.Introduction to the particular problem

Wikipedia (2005) defines privacy as the ability of an individual or group to stop information about themselves from becoming known to people other than those they

choose to give the information to (it also defines the condition of being left alone). Moreover, Koneya (1977) defines privacy as the right individuals have to control what information about themselves should or should not be communicated to others and under what circumstances.

Section 14 of the South African Constitution of 1996 (Steyn, 2004) states that "everybody has the right to privacy, which includes the right not to have:

- Their person or home searched;
- Their property searched;
- Their possession seized; or
- The privacy of their communication infringed".

Section 32 of the same constitution states, "everyone has the right of access to

- Any information held by the state, and
- Any information that is held by another person and that is required for the exercise or protection of any right"[1].

Despite the high level of security offered by biometrics technologies, there have been growing concerns related to privacy. Privacy associated with biometrics has become an important topic of discussion. There is a concern relating to the collection, storage, use, and disclosure of an individual's personal biometric information. Some believe that biometrics leads to the invasion of privacy, but others differ. According to Davis (1994) several countries, including Australia, Canada, the United States and New Zealand, have witnessed public disquiet over certain identification schemes. This

[1] http://www.concourt.org.za

raises the need to investigate South African opinions regarding the use of biometrics authentication, with the focus on the informational privacy.

Informational privacy is creating most of today's controversy, as personal information is being collected and could be used by businesses day-in and day-out to gain competitive advantage.

For this research, the privacy-related concern is mainly centred on informational privacy. There are many factors that lead to informational privacy, such as:

1. Accuracy - The problems with the biometrics systems are the False Acceptance Rate (FAR) and False Rejection Rate (FRR). Biometric systems will sometimes mistakenly accept an impostor, that is, falsely accept an impostor as a valid individual or conversely, reject a valid individual, that is, falsely reject a genuine person (Jain, Hong & Pankanti, 2000).
2. Function Creep - function creep refers to the dangers of finding biometric data exchanged without consent, within the biometric community (Langenderfer & Linnhoff, 2005).
3. Identity theft - Identity theft is the act of obtaining personal information without the concerned person's consent (Friedewald, Vildjiounaite, Punie and Wright, 2006).

The above-mentioned factors will be described in more detail in chapter 4, Biometrics and Privacy.

1.7.Scope

For this research, 150 air travellers (or passengers), from the City of Cape Town, South Africa, were selected from various travel agencies, and interviewed. During these interviews a survey questionnaire, based on the literature, was administered. It contained close-ended questions on a 6-point Likert scale (1 = Totally Disagree, 2 = Mostly Disagree, 3 = Sometimes Disagree, 4 = Sometimes Agree, 5 = Mostly Agree, 6 = Totally Agree). Additional provision was also made for a respondent to select a "statement not relevant" option. It focused on security and privacy aspects of possible biometrics' application at Cape Town Airport.

1.8.Research questions

This research will primarily address the following questions:

- Will travellers accept biometrics for higher security measures, that is, positive authentication?
- Will passengers be willing to opt for higher security measures by giving up privacy?
- Are passengers prepared to make privacy sacrifices for the sake of convenience?

1.9.Theoretical framework

The explosive growth of information system technology has led to the development of both larger and more sophisticated information systems (Jackson, Chow and Leitch, 1997). IT plays a role in many, if not most of, everyday operations of today's business world to process data, gather information, store collected materials, accumulate

knowledge, and expedite communications (Chan, 2000). IT roles according to Chan (2000) can be defined as initiators, facilitators, and enablers where:

- Initiator – acts as an agent of change;
- Facilitator – may serve as something to make work or workload easier;
- Enabler – something that offers the ability or necessary assistance to accomplish something.

These significant roles played by information technology in an organisation can create new needs, cause new product development, and command new procedures. In spite of the effective and efficient deployment of IT, one must keep in mind that the human elements, issues of personality, culture, and society, also play major roles in organisational operations (Chan, 2000).

Information technology adoption and use remains a central concern of information system research and practice. In the past, information technology (IT) research had long centred on the invention, implementation, and implications of computer technologies at various levels (Venkatesh & Davis, 2000). However, during the past couple of years the focus has also moved towards the users' acceptance of IT. These abovementioned authors believe that significant progress has been made in explaining and predicting user acceptance of information technology.

The fundamental determinants of user acceptance of information technology identified by Adams, Nelson and Todd (1992) were perceived usefulness and perceived ease of use. Perceived usefulness is defined as "the degree to which a person believes that using a particular system would enhance his or her job

performance" (Davis, 1989). Perceived ease of use refers to "the degree to which a person believes that using a particular system would be free of effort" (Davis, 1989). Several theoretical models have also been proposed to explain end-user acceptance behaviour towards technology (Ma & Liu, 2004). The Technology Acceptance Model (TAM), introduced by Davis, is one of the most widely used models to explain user acceptance behaviour (Ma & Liu, 2004). Legris, Ingham and Collerette (2001) indicate that TAM is a useful model that examines the mediating role of perceived ease of use and perceived usefulness.

As revealed by Amberg *et al.*. (2005), TAM and other models (as discussed below), claim to be applicable to the evaluation of Information Systems in general. However, an integrated model shows superiority over basic models. Özel, Çilingir and Erkan (2006) suggested that there are two main classes of acceptance models:

- Basic models, and the
- Integrated models.

The basic models denote approaches which are mainly founded in intentional models originated in social research. Examples of such models are (Özel, Çilingir & Erkan, 2006):

- Theory of Reasoned Action (TRA),
- Technology Acceptance Model (TAM),
- Theory of Planned Behaviour (TBP),
- Task-Technology-Fit model (TTF), and
- Diffusion of Innovation (DoI) theory.

As for the integrated models (cited in Özel, Çilingir & Erkan, 2006), they are built mostly on a combination of basic models. The acceptance model of Taylor and Todd, which is built on the integration of TAM and TBP, The Unified Theory of Acceptance and Use of Technology (UTAUT) by Venkatesh *et al.*., and finally Dynamic Acceptance model for the Re-evaluation of Technologies (DART) by Amberg *et al.*., an integration of concepts of five existing acceptance models including TAM and TTF.

The acceptance of biometrics technology from users' perspectives for this research will be assessed using DART, with the focus on privacy and security. DART is an instrument specially designed for the analysing and the evaluating of the user acceptance of innovative technology or products (Amberg, Fischer and Schröder, 2005). DART was first introduced by Amberg, Hirschmeier and Wehrmann, (cited in Amberg *et al.*, 2005). Bente, Surakka, Lylykangas, Vuorinen, Troitzsch, Eschenburg and Krämer (2005), distinguish two orthogonal bipolar evaluation categories from the DART model:

- "Benefits" and "Efforts" comprise all positive and negative facets of the user acceptance;
- "Products and Services" (Internet applications) and "Contextual Conditions of Products and Services" include basic socio-cultural and economic conditions, which also have a considerable impact on user acceptance.

From these categories the authors derive four dimensions that are relevant for an analysis of user-acceptance (Bente *et al.*, 2005):

- Perceived ease of use;

- Perceived usefulness;
- Perceived network effects; and
- Perceived costs.

These four dimensions focus on the subjective perception which emphasizes the valuation of a product or service by the end user's subjective point of view (Amberg *et al.*, 2005).

Biometrics is an emerging technology and for the research the focus will be to measure the behavioural intentions of users regarding biometric technology. Thus, the abovementioned four dimensions can be explained with reference to biometrics (Bente *et al.*, 2005):

- The dimension "perceived network effects" refers to the contextual conditions of a product, for example, compatibility, dissemination, level of awareness or popularity.
- The dimension "perceived ease of use" refers to the "degree to which a person believes that using a particular system would be free of error" which mainly links to usability aspects as learnability, ease of enrolment and login procedure.
- The dimension "perceived usefulness" covers aspects as security and reliability of biometrics as well as usability related issues, for example, convenience, quickness and fun.
- The dimension "perceived costs" is related to different kinds of costs, such as installation and material costs as well as non material cost (for example, giving up some privacy).

Therefore, Bente *et al.* (2005) suggest that the DART model proves to be a suitable frame of reference to review the existing literature regarding user acceptance in the field of biometrics and security applications.

1.10.Impact of survey research

The survey research could impact upon The Airport Company of South Africa (ACSA) and the travellers.

ACSA

An organisation's investment in information technology to support planning, decision making, transaction processing and communication is often very large and risky (Jackson, Chow and Leitch, 1997). In order to develop a contemporary system, the challenge is to effectively satisfy and increase prospective users' intentions to use a new system.

In order to examine and control the range of factors that are likely to lead to the behavioural intention to use an information system (Jackson, Chow and Leitch, 1997) this research may help information system management to have an understanding of users' perceptions of integrating biometrics at the Cape Town airport.

This research may also provide ACSA with important information for the introduction of biometrics at airports and also assist in the determination of what is important to the passengers. Moreover, according to Jackson and Chow (1997), it is imperative that system developers enhance their understanding of users' behaviour regarding new

technologies so as to make proactive decisions to foster the adoption and effective use of the new systems.

Travellers

As for passengers, safety at the airport is of paramount importance. The number of passengers visiting South Africa will increase substantially due to the 2010 World Cup Soccer Tournament to be held in South Africa (Dlamini, 2005). Thus, improving the security at the airport will help increase the safety of such visitors.

1.11.Literature review

A preliminary literature study reveals two lobby groups regarding the use of biometrics. There are those who speak in favour of biometric authentications, and others who argue against the use of biometrics technologies because of concerns related to privacy.

As shown in Figure 1: Research Context, below (developed from this proposal's literature study), there are two key areas that the research focuses on, that is, privacy and security in the airport security. In the context of airports, biometrics is used as a process tool to authenticate travellers, and identify possible terrorists in order to prevent interference to the normal airport operation.

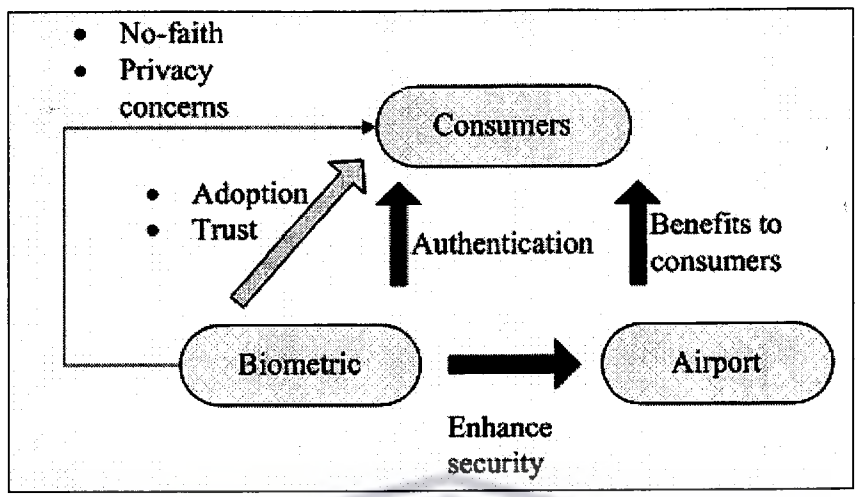


Figure 1: Research Context

With respect to the use of biometrics at airports, privacy opponents believe that biometrics can be used to enhance security, and that they offer greater convenience than traditional methods of authentication such as passwords and card keys.

The types of authentication tools that are currently in use are:

- Something the traveller knows such as a password,
- Something the traveller possesses, for example, a passport or valid drivers' license; and,
- Something the traveller is, that is, a physical characteristic lending itself to biometric measures.

Ratha, Connell and Bolle (2001) claim that automated biometrics in general, and fingerprint technology in particular, may provide a much more accurate and reliable user authentication method. Moreover, Doggett (2002) states that the majority of US citizens are happy to use biometrics in their daily life, with more than 70% in favour of carrying identification cards with fingerprints.

Alternatively, privacy advocates are against the use of biometrics authentication. The two major privacy concerns are informational privacy and physical privacy.

Firstly, pertaining to informational privacy, there is the fear of "function creep", theft and misuse of personal data. According to Langenderfer and Linnhoff (2005), function creep refers to the dangers of finding biometric data exchanged without consent, within the biometric community. Due to the widespread use of biometrics technologies, individuals are reluctant to divulge their personal characteristics to organisations because of increasing concerns over the confidentiality of their information. "Databases of biometric information can be misused if they fall into the wrong hands. Many security, law-enforcement, border-control, medical, and banking organisation maintain vast biometrics databases that are available to government agencies and business entities" (Allen, 2005).

Biometric information is considered as personal and sensitive because if it is captured by a third party or unauthorised people it is not easy to replace. "The problem with biometric authentication is the re-issuance of identity tokens. For authentication based on physical possessions, for example, keys, a token, can be easily cancelled and the user reassigned new ones. Similarly, a password can be changed. An individual, however, has only limited biometrics and this immediately raises privacy concerns about misuse of this information" (Ratha *et al.*, 2001).

In addition, with regard to physical privacy, there are concerns about stigmatization, actual harm and hygiene. The storage of unique human characteristics, especially fingerprints in a central database, can raise doubt over the use of biometrics

authentication, as fingerprints are used by police officers to track criminals. Therefore, many individuals find it a loss of dignity if their biometrics template is stored in the same database as that of criminals. People may also feel uncomfortable using the same sensor that has been used by thousands of individuals. Finally, there is a concern that biometrics may cause physical harm. Langenderfer and Linnhoff (2005) suggest that although the retina is a highly distinctive biological feature and thus a potentially useful measurement target, retina scans are highly intrusive and there is some concern that direct laser scanning of retinal tissue can, over time, result in damage to the eye.

1.12.Research methodology

To meet the research objectives, research in the form of a quantitative questionnaire survey will be carried out. The survey questionnaire will be developed based on the literature review. The research process, reliability check, validity check, pilot test, research methods, methods to avoid biases, and sample size are described in detail below.

1.12.1. Research process

The research for this study can be referred to as descriptive research. Sekaran (2000) suggests that a descriptive study is undertaken in order to ascertain and be able to describe the characteristics of the variables of interest in a situation. The variables in this study include security and individuals' right to privacy regarding biometrics in airports. "Descriptive studies that present data in a meaningful form thus help to:

- Understand the characteristics of a group in a given situation,
- Think systematically about aspects in a given situation,

- Offer ideas for further probe and research" (Sekaran, 2000, 126).

Thus, for the purpose of this research, a survey questionnaire, see APPENDIX 1: Questionnaire, is considered a useful tool to gather primary data from travellers. It is important to develop a survey instrument unique to this research because of the several areas it deals with. The instrument in this study will be administered in the form of a 6-point Likert scale, with additional provision made for a respondent to select a "statement not relevant" option similar to the one used by Mansfield (2005) in his research.

1.12.2. Reliability Check

As for a reliability test, Cronbach's Alpha statistic is the most frequently used indicator of instrument reliability in survey research (Kivela *et al.*, 1999). Another way of testing the reliability of data obtained is indicated by Smith (1972:25) where the same questions can be asked of the same respondent by different interviewers and the results compared.

1.12.3. Validity Check

In order to evaluate the validity of the questionnaire, a pilot test was conducted with 10 randomly selected respondents. In addition, it was evaluated by a group of experts to solicit comments and suggestions about the instrument, and to assess the duration of a survey questionnaire in order to determine the average time for completing the questionnaire.

1.12.4. Pre-test or Pilot test

As McClelland (1994) indicated, a draft questionnaire should be subjected to a pre-test in which it is proofread for typographical errors, vague and/or misleading statements, and neutral phrasing as it serves to establish the framework for validity and reliability. Once the questionnaire has been tested, proofread and finalized, it will be pilot tested by a group of travellers.

1.12.5. Research method

To gather primary data the research methods for this survey will be by means of self-administered questionnaires.

1.12.6. Avoiding bias

Firstly, in order to avoid bias, the data collection part of the survey that will be carried out will be focused on international air passengers. The reason for such a choice is that such passengers usually have the requisite broad international experience.

1.13. Research hypotheses

The data collected during the survey will be analyzed and used to test the hypotheses. Three hypotheses are drawn to investigate the travellers' opinion regarding acceptance, privacy concerns and convenience vis-à-vis biometrics application. Null hypothesis is denoted by H_0, whereas the alternate hypothesis is symbolized by H_1. For each of the statements mentioned below, respondents will be asked to express their opinion regarding issues surrounding biometrics. If respondents indicate a high level of agreement then the null hypothesis is accepted. Otherwise the null hypothesis is rejected for the alternate hypothesis.

As shown in Table 1: Hypotheses Variables, the independent variables, that is, the likely cause of change in the dependent variable, are:

- In the first hypothesis: biometric security measures
- In the second hypothesis: Privacy
- In the third hypothesis: Privacy.

Hypothesis number	1	2	3
Independent variable	biometric security measures	Privacy	Privacy
Dependent variable	Travellers' attitude	Higher security	Convenience

Table 1: Hypotheses Variables

The dependent variables, that is, the variable being studied, are:

- In the first hypothesis: Travellers' attitude
- In the second hypothesis: Higher security
- In the third hypothesis: Convenience.

Hypothesis 1

H_0 - Biometric security measures at airports are positively accepted by travellers.

H_1 – Biometric security measures at airports are not accepted by travellers.

Biometrics is gaining acceptance in many fields. The H_0 hypothesis states that the use of biometrics for higher security at the airport is positively accepted by travellers. Whereas H_1 hypothesis testifies that people have negative opinions concerning the application of biometrics at the airport.

Hypothesis 2

H_0 - Passengers will sacrifice privacy for higher security.

H_1 – Passengers will not sacrifice privacy for higher security.

Biometrics can pose a threat to personal privacy. The H_0 hypothesis states that despite privacy concerns, travellers are prepared to sacrifice personal privacy for a high level of personal security at the airports. The H_1 hypothesis affirms that privacy is more important to the passengers than security.

Hypothesis 3

H_0 - Passengers will sacrifice privacy for convenience.

H_1 – Passengers will not sacrifice privacy for convenience.

Biometrics raise privacy concerns more now than ever before. However the null hypothesis maintains that passengers will report that privacy is less important than pleasure features (convenience, ease of use) in using biometrics, thus they are willing to sacrifice privacy for convenience.

Definitions

The word "recognition" will be used throughout this research so that a distinction is made between identification and verification. However, identification refers to comparing the captured biometrics characteristics with the individual's biometrics template, which is pre-stored in the system database. Verification, for example, involves comparing a live biometric with a stored template that is on a smart card.

Also, Travellers, Passengers, and Respondents are used interchangeably in this research.

1.14.Structure of the thesis

The thesis is divided into seven chapters:

Chapter 1: In this chapter the research context, rationale of the study, research questions and the literature review are discussed. Then research methods and hypotheses are presented. Finally, the assumption and limitation, and the thesis structure are shown.

Chapter 2: In this chapter the general idea of border security of airports prior to September 11, 2001, and history of terrorism will be presented. After that, the September 11, 2001, terrorists attack will be mentioned. Then, technologies used to enhance security at airports will be pointed out. The impact of biometrics authentication on the border security of airports after September 11, 2001 will be illustrated.

Chapter 3: The definition of biometrics, different types of biometrics, the biometric system and biometric feature will be presented in this chapter. The differences between identification and verification will be highlighted.

Chapter 4: This chapter will illustrate the main reasons for privacy concerns related to biometrics in the border security of airports.

Chapter 5: Research Methodology: this chapter describes the methodology used to collect data and its examination. Data will be collected by means of questionnaires

from Travel agencies and airline travellers residing in the City of Cape Town in South Africa. Data is then analysed and results presented.

Chapter 6: This chapter will consist of the findings and analyses of the data collection of individuals' attitudes towards security and privacy of biometrics at Cape Town (CT) Airport.

Chapter 7: Conclusion – This chapter summarises the research findings and recommendation for future research.

1.15.Conclusion

This first chapter introduced the background and context of the study. It is suggested that biometrics offers greater security and convenience than traditional methods of personal recognition for airport security. However, it also described the problems associated with biometrics technology. The concerns raised by biometrics involve the unauthorised use, collection, storage, and disclosure of personal biometrics information.

This chapter has introduced the aims, research problems, and hypotheses of the study and outlined the appropriate methodology used to seek answers to the questions.

It has been mentioned in this chapter how a survey questionnaire, used for research was developed and used to collect information about travellers' opinions regarding privacy and security. In addition, all the factors are taken into consideration to design an effective questionnaire, such as reliability and validity checks.

The next chapter is the first of three that introduce the literature relating to different aspects of biometric applications. This chapter discusses airport security. The two following chapters review the literature on biometrics, and then security and privacy. Baggage screening, passenger screening, and access control are illustrated in depth as it shows that terrorists can take advantage of these areas and use fake passports to circumvent the security check with harmful objects to get on a plane.

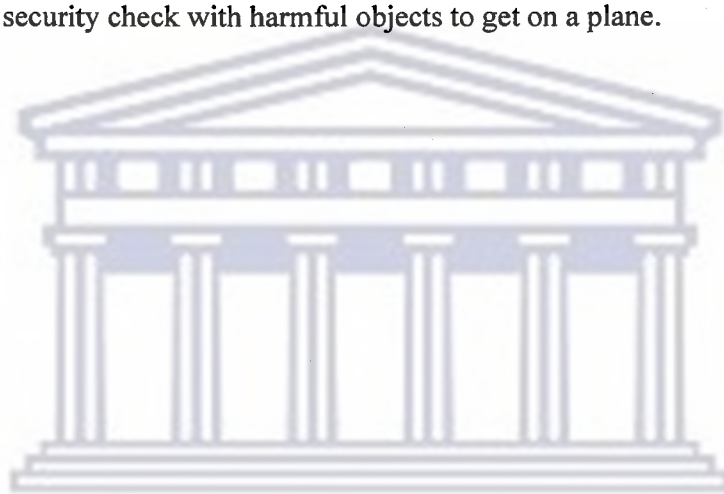
CHAPTER 2: AIRPORT SECURITY

2. Introduction

This chapter gives an overview of a generic airport and the security at the airport, and includes material from the literature. In order to create the context for this study with the focus on the relationship between security and the privacy of individual it is important to review the procedures followed at major airports. Airport security has gained paramount importance regarding the safety of their travellers in the past few decades. Airports are recognizing that their key responsibility is the protection of travellers, preventing the introduction of explosives and dangerous weapons being carried onboard airplanes due to increased superiority of terrorists, and improved access control, enhancing passenger and luggage screening.

This chapter also discusses the implications of terrorism on every individual's life as hijacked airplanes in the past have murdered and otherwise affected the lives of many people, since explosives are easily introduced by terrorists during the different steps of luggage handling. In addition, in this chapter, screening of passengers is discussed that prevents unauthorised travellers from having access to sterile areas of the airport. The process through which a traveller moves from the vehicle parking area to the different security areas before getting onboard an airplane is also described. Terrorism has changed the travelling experience of individuals for ever.

The next chapter is the first of three that introduce the literature relating to different aspects of biometric applications. This chapter discusses airport security. The two following chapters review the literature on biometrics, and then security and privacy. Baggage screening, passenger screening, and access control are illustrated in depth as it shows that terrorists can take advantage of these areas and use fake passports to circumvent the security check with harmful objects to get on a plane.



CHAPTER 2: AIRPORT SECURITY

2. Introduction

This chapter gives an overview of a generic airport and the security at the airport, and includes material from the literature. In order to create the context for this study with the focus on the relationship between security and the privacy of individual it is important to review the procedures followed at major airports. Airport security has gained paramount importance regarding the safety of their travellers in the past few decades. Airports are recognizing that their key responsibility is the protection of travellers, preventing the introduction of explosives and dangerous weapons being carried onboard airplanes due to increased superiority of terrorists, and improved access control, enhancing passenger and luggage screening.

This chapter also discusses the implications of terrorism on every individual's life as hijacked airplanes in the past have murdered and otherwise affected the lives of many people, since explosives are easily introduced by terrorists during the different steps of luggage handling. In addition, in this chapter, screening of passengers is discussed that prevents unauthorised travellers from having access to sterile areas of the airport. The process through which a traveller moves from the vehicle parking area to the different security areas before getting onboard an airplane is also described. Terrorism has changed the travelling experience of individuals for ever.

2.1. Identifying Terrorists

The US State Department defines terrorism as "premeditated, politically motivated violence perpetuated against non-combatant targets by sub-national groups or clandestine agents, usually intended to influence an audience" (Kondrasuk, 2005). In addition, The US Federal Bureau of Investigation (FBI) defines terrorism as the unlawful use of force or violence against persons or property to force the terrorists' political or social views onto a government or its citizens to influence them to change in some way (Kondrasuk, 2004). Terrorism is widespread and seen as a problem throughout the world, including South Africa, where suspected terrorists within the borders were arrested (Kondrasuk, 2005).

According to Askew (cited in Yoo & Choi, 2005), the first hijacking occurred in the early 1930s when the aviation industry was in its infancy. It is estimated that there were over 364 hijackings worldwide between 1968 and 1972.

Novakoff mentioned that (cited in Singh & Singh, 2003), from 1985 to 1997, eight commercial aircraft have been lost or damaged due to suspected terrorist bombings and about 1100 people died in these tragedies. The cost in human lives has been enormous. Many of these incidents were exacerbated by the lack of suitable security controls. For example:

- On June 23, 1985, Air India Boeing 747 crashed into sea as a result of the explosion in the cargo hold.
- On November 29, 1987, Korean Air Flight 858 was destroyed from an explosive device inside the cabin.

- On December 21, 1988, PanAm flight 103 was destroyed by a 12 ounce bomb hidden in a portable radio over Lockerbie, Scotland.
- On September 19, 1989 an UTA flight was destroyed over the Sahara from an explosion in the forward cargo component of a DC-10 aircraft.
- On November 27, 1989, an Aviance Boeing 727 was destroyed by an explosive device in the cabin.
- On July 17, 1984, an Alas Chiricanas Airline EMB-110 crashed from a bomb explosion in the cabin during a flight from Colon City to Panama City.
- On December 11, 1994 a Philippine Airlines Boeing 727 was attacked in flight from a bomb explosion in the cabin.
- On July 9, 1997, an explosive device in the passenger cabin detonated on a Transporte Aereo Mercosur Fokker 100 during flight.

The large number of airline bombings shows the real threat to the air passenger travel and as a result of the serious breaches of security in the past, research into advanced screening equipment and associated technologies have become a priority (Singh & Singh, 2002). The airport security has become a focal point for passenger safety.

2.2. Airport Security

According to Stibbe (2005), the past decade aviation has inspired the technological process. The focus has changed from an emphasis on price, speed and security of aircraft, to security and the efficient movement of people. The focus and scope of this investigation is Cape Town. CT International Airport was believed to be one of the safest airports in the world. However, recently a Zimbabwean student from the University of Cape Town (UCT) tried to hijack a plane from CT with syringe. Therefore, with the likely increase in the number of passengers for the 2010 World

Cup Soccer Tournament, which will be held in South Africa (Dlamini, 2005), there is a need to improve the security at the airport and more attention is needed to maintain the safety of the travellers.

Airports are a crucial component of the physical infrastructure for the airline industry (Coughlin, Cohen & Khan, 2002). A distinction needs to be made between airports and airlines activities as many people often get confused with these terms. Airports act as providers of the on-ground infrastructure for flight operations while airlines offer the transportation services.

The core tasks of an airport, in the narrow engineering sense, are the supply, maintenance and protection of the infrastructure that is necessary for landing, starting, taxiing and parking of airplanes. In its full social and commercial sense, its role is to facilitate the link between passengers arriving by car, taxi and other modes and their access to aircraft. Additionally, the airport provides facilities such as terminals, gates and maintenance facilities which are essential for the completion of flight operations, and which facilitate the access to energy, water or fuel for the aircraft.

Figure 2, illustrates the primary and supporting activities for a generic airport. The concept of the value chain was developed by Porter (1985) and offers a useful way to grasp the strategically relevant activities that are important to successful partners involving airport companies.

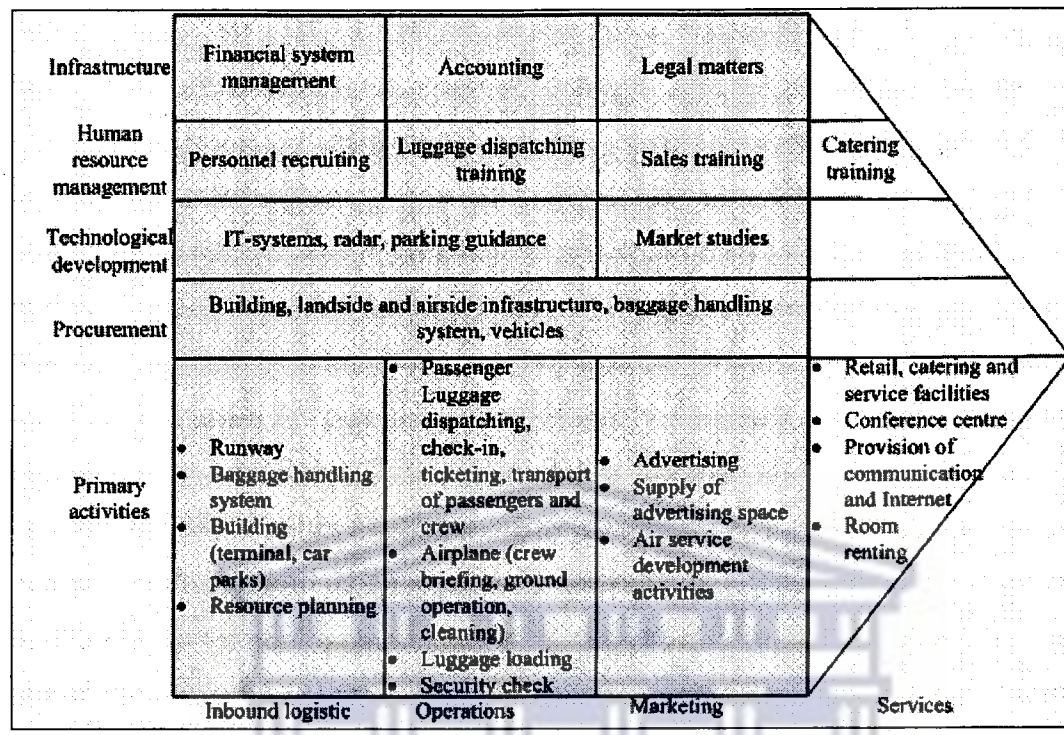


Figure 2: The value chain of an airport Source (Albers *et al.*, 2005)

In the value chain, airports' primary activities are distinguished from the support activities.

1. The generic primary activities identified by Porter include:
   I. Inbound logistics;
   II. Operations;
   III. Outbound logistics;
   IV. Marketing and sale; and
   V. Services.
2. The support activities are those that enable the performance of the primary activities and include:
   I. Procurement
   II. Human resource management
   III. Technological development, and

IV. Infrastructure.

For the purpose of this research, special attention will be set onto the primary activity of operations since it includes:

- Security checks;
- Passenger screening, such as luggage dispatching, check-in, ticketing, transport of passengers and crew;
- Airplane – crew briefing, ground operations and cleaning;
- Ramps or Luggage – loading and unloading of the airplane and luggage transfer.

There is a perceived need to protect passengers following the terrorists' attacks in the past. Among the plethora of terrorist attacks on airline industry, some of the ones that made headline news are (Tzannatos, 2003):

- The hijacking of the French airplane which ended at Entebbe Airport in 1976;
- The hijacking of the four US airplanes in the USA and their transforming into guided missiles on 11 September 2001.

For many airports, commercial activities are central to their future economic viability and a pre-requisite to growth (Torres, Dominguez, Valdes & Aza, 2005). Since security consideration influence demand patterns, airports are treating safety arrangements within their primary activity operations to protect passengers and buildings (Albers *et al.*, 2005). Therefore the responsibility for improving airport security remains the duty of both the airlines and the airport.

2.3. Security at airport prior to the 9/11 event

Generally speaking, providing security has been the responsibility of air carriers and airports (Coughlin, Cohen & Khan, 2002). The airlines are responsible for passenger and baggage screening, both carry-on and checked. The airlines are also responsible for security from the screening check-point to the aircraft (Coughlin, Cohen & Khan, 2002). Airports are responsible for law enforcement and general security in the airport vicinity, including exterior areas, parking areas, the airport perimeter, and interior areas up to the security checkpoints (Coughlin, Cohen & Khan, 2002). Another key area is access control.

2.3.1. Access Control

Access control is the process of screening people and baggage in order to detect and prevent entry of unauthorised personnel, firearms or explosives into the airport area and aircraft (Babu, Batta & Lin, 2006).

Sophisticated instruments and trained personnel are the means to screen the passengers or items passing through the various checkpoints at the access control system at airports (Babu *et al.*, 2006). Hogan pointed out, (cited in Babu *et al.*, 2006), that some of the important check stations at typical airports are:

1. Check in;
2. International area;
3. Boarding area;
4. Boarding gate;
5. Luggage check in;
6. Customs checking station; and

7. Explosives and drug interdiction and control station.

The control tower and airside are secured areas where access is strictly controlled (Stibbe, 2005). The area with the highest focus on security, however, became that involving the passenger.

2.3.2. Passenger and baggage screening

Anderson points out, (cited in Turney, Bishop & Fitzgerald, 2004), that prior to entering the gate area, passengers must pass through metal detecting devices and subject their carry-on bags to examination through an X-ray machine. Also, Tyson and Grabianowski (2002) state that all the public access to an airport is channelled through the terminal where every person must walk through a metal detector in order to identify any targeted object. If a suspicious item is found, then the person is asked to remove all metal objects and step through the metal detector again. If the metal detector continues to indicate the presence of metal, the attendant uses a handheld detector to isolate the cause.

2.3.3. Baggage handling and screening

The section below discusses the baggage handling and baggage and passenger screening procedures that are currently in place at the airports.

2.3.3.1. Baggage handling

The process of baggage handling starts by receiving luggage from travellers at the ticketing counter (Abdelghany, Abdelghany & Narasimhan, 2006). Each received piece of luggage is given an identification tag that indicates its itinerary and a unique bar code and is then sent to the baggage-handling facility. Similarly, luggage pieces

that arrive at the airport are also received and transported to the baggage-handling facility.

In summary, baggage handling at an airport usually involves three main functions (Abdelghany *et al.*, 2006):

- Moving bags from the check-in area to the departure gates,
- Transferring bags from one gate to another, and
- Moving bags from arrival gates to the baggage-claim area.

Due to security breaches in the past, terrorists can easily introduce explosives during the different steps of luggage handling process.

2.3.3.2. Baggage Screening

According to Yoo and Choi (2005), the X-ray machine in service at airports for passenger carry-on luggage is slightly outdated. The screeners complain that the image on the X-ray monitor is too small to easily identify items in the luggage.

2.3.3.3. Passenger Screening

It is quite common for explosives, weapons or drugs to be concealed on the passenger. The technologies that are used for scanning luggage cannot be used for screening passengers, for health reasons (Singh & Singh, 2002). Passenger screening is a huge problem as:

- Passengers and airlines want short lines and quick service but law enforcement has other priorities which creates a point of friction between the commercial and law enforcement aspects of aviation (Stibbe, 2005).

- A screening solution must not only be accurate, but also publicly acceptable (Singh & Singh, 2002). Popular methods of passenger screening to date include walk-through metal detectors, metal detector hand wands and pat-down searches. According to Singh and Singh (2002), emerging technologies are based on either imaging or trace detection and can see through the clothing and produce an image of the human body and concealed items underneath. While strip-searching is one of the best methods, it is not always possible to search everywhere (Singh & Singh, 2002). However seeing through the clothing or strip-searching can be a cause of major concern among travellers.
- In addition, according to Yoo and Choi (2005), a universal technical problem for airport security officials all over the world is with the hand-held metal detectors. The screening personnel are frequently annoyed by the acutely sensitive responses from the detectors to very small metal parts or by acutely loud or weak beeping sounds from the alarm (Yoo & Choi, 2005).

Moreover, according to the survey conducted by Yoo and Choi (2005), the obstacle in effective passenger screening can be grouped in three different groups involving:

1. Human resources
    - Short employment period of screeners because of a high rate of labour turnover,
    - Insufficient training,
    - Screeners' mental and physical fatigue because of high work load during peak hours,
    - Low wages for screeners,
    - Insufficient quantity of human resources.

2. Facility and equipment
    - Low quality screening equipment,
    - Inadequate space at screening checkpoints.
3. Work procedures and responsibility
    - Unreasonable handling procedure for certain prohibited items detected at screening points,
    - Uneven distribution of passengers sent to available screening checkpoints,
    - Pressure from both the airport operation department and the airlines against any delays caused by the passenger screening process.

2.4. The role of technology in Airport Security

The air transport system is without question a target for terrorist groups as airport bombings gain terrorist groups highly coveted publicity (Lewis, Curt, Montgomery & John, 1989).

According to Heracleous and Wirtz (2006), biometrics offer significant security enhancement as well as other value-added applications. Some examples where biometrics are currently used are:

- At Heathrow Airport in the United Kingdom, iris recognition is being used to check the identity of air passengers and allow automatic entry into the country for a selected group of travellers, bypassing the need to present passports, and speeding up the entry process whilst maintaining security (Connolly, 2006).
- In Canada, iris recognition is used to verify the identity of frequent travellers, using an ordinary digital camera, within about 2 seconds without the passenger having to remove spectacles or contact lenses (Connolly, 2006).

- Changi Airport, in Singapore, together with Singapore Airlines are employing biometric technologies to offer every traveller's dream when it comes to airport procedure: the ability to breeze through airline check-in, security checks as well as immigration checks in less than one minute, all within a context of enhanced travel security (Heracleous and Wirtz, 2006).

Published in Postnote (2001), the areas where biometrics could be used in airports to enhance security include:

- Confirming that a passenger boarding a plane is the same individual who checked in. Passengers would be asked to agree to a biometric scan at check-in and again at the gate.
- Controlling access to restricted areas. This would apply to staff, who would gain access to building either through demonstrating that they matched the biometrics stored on their card or through comparison with a database.
- Identifying known terrorists or criminals. Biometrics would be scanned from people passing through airports and compared with a database of known criminals or terrorists.

2.5. Conclusion

This chapter discussed airport security at the airport prior to September 11, 2001 and showed the negative impact of terrorism on aviation security from that date. The Airport Company of South Africa (ACSA) recognized the need for enhanced security by integrating state-of-the-art and sophisticated technology in order to combat future terrorist attacks. In order to deal with the problems of security at airport, they have

and are implementing better scanning and biometric technologies that can check luggage and authenticate travellers properly.

CHAPTER 3: OVERVIEW OF BIOMETRICS

3. Introduction

The emerging use of biometric technology, especially in security applications, is expanding rapidly particularly in the light of the September 11, 2001 attacks. It is important to review biometrics in security because it is regarded as a possible solution to combat terrorism and improve security by controlling access to highly secure areas at airports. This chapter therefore represents an overview of Biometrics systems from the literature that accurately assesses its capabilities and usefulness in airport security. The history and definition will show that biometrics is not something new but has existed for many centuries. The difference between identification and verification will also be discussed as there are two ways to determine the identity of a person.

This chapter gives a brief description of how a biometric system works and introduces the different types of biometrics based technologies that are currently present on the market. After describing the characteristics of the system, the chapter is concluded with different types of errors, such as False Acceptance Rate and False Rejection rate that are associated with the system that allows an unauthorised person, and also prevents an authorized from accessing the system.

So the first question that needs to be asked is: What is biometrics?

3.1.Definition

Biometrics can be defined as the measurable characteristics of an individual based on his or her physiological features or behavioural patterns that can be used to recognize or verify his or her identity (Bennett, 2000). Kochan (2004) defines biometrics as the "automated identification or verification of human identity through the measurement of repeatable physiological and behavioural characteristics".

Theoretically, installing biometrics can be very effective for increasing and improving security at the airports in comparison to the traditional method of authentication, such as the use of passports. Thus, getting a better understanding of the different types of authentication is important.

3.2.Types of Authentication Techniques

The widespread use of biometrics-based identification and authentication systems has been considered in many applications in recent years (Zorkadis & Donos, 2004). However, the three traditional methods of user authentication by which a user can prove their claimed identity are (Liu & Silverman, 2001):

1. Something the user knows – a password, PIN, or piece of personal information (such as mother's maiden name);
2. Something the user has – a card key, smart card, or token; or
3. Something the user is – a biometric, fingerprint, iris, retina and hand geometry.

All passengers travelling internationally and those applying for driver's licenses are familiar with fingerprint technology. They need to provide fingerprints before

receiving their passport and driver's license. But, the most widespread form of user authentication is based upon 'something the user knows', for example, passwords used at ATM machines to withdraw cash. Such techniques include (Caelli, Longley & Shain, 1994:465):

1. Passwords;
2. Pass-phrases;
3. PIN (Personal Identification Numbers); and
4. PIC (Personal Identification Codes).

Nonetheless, security can be easily breached in a security system that uses passwords, when the latter is divulged to an unauthorised user or a badge is stolen by an impostor (Ross & Jain, 2003). The emergence of biometrics has gome some way to address these problems that plague traditional verification methods (Ross & Jain, 2003). A biometric, at least something the user is, is the most secure and convenient authentication tool. It can not be borrowed, stolen, or forgotten, and forging one is practically impossible (Liu & Silverman, 2001). Biometrics may sound like a recent technology, but in reality it has existed for thousands of years.

3.3.History of biometrics

The term "biometrics" is derived from the Greek words "bio", meaning life, and "metric", signifying to measure (Scherer, 2005). Thousands of years ago, biometric verification was employed routinely by people from the Nile Valley in a number of business situations. Individuals were formally identified via unique physiological parameters such as a scar, measured physical criteria or a combination of features such as complexion, eye colour, height and so on. Also, the basic principles of

identifying the unique physiological parameters of individuals were used in the legal proceedings and agricultural sectors, where grain and provisions were supplied to a central repository though the number of individuals being dealt with was not as many as it is now. Thus there was no need for electronic biometric readers and computer networks (Ashbourn, 1999).

In the 14th century, Chinese merchants used biometrics to stamp children's palm prints and footprints on paper with ink in order to distinguish the young children from one another (Scherer, 2005). In the mid 19th century; in France, Bertillon, the chief of the criminal identification division of the police department, developed and then practiced the idea of using various body measurements (for example, height, length of arms, feet, and fingers) to identify criminals. In the late 19th century, just as his idea was gaining popularity, it was eclipsed by a far more significant and practical discovery: the distinctiveness of human fingerprints. Soon after this discovery the idea of "booking" criminals' fingerprints and storing them in databases (initially, card files) was used. Later, police gained the ability to "lift" leftover, typically fragmentary, fingerprints from crime scenes (commonly called latents) and match them with fingerprints in the database to determine criminal's identities (Prabhakar, Pankanti & Jain, 2003).

After that, individuals and organisations both in the military and commercial sectors used electronics and microprocessors to automate identity verification. So, various projects were initiated related to biometrics that eventually led to a large, ungainly hand-geometry reader being produced. The geometry reader was further enhanced by

a group of small specialist companies into a much smaller device which worked well and found favour in numerous biometric projects around the world (Ashbourn, 1999).

Since then other biometric technologies have been produced and refined so that they would become reliable, easily-deployed devices (Ashbourn, 1999). The first system for classification of fingerprints by their patterns, was described in 1684 by a Dr Nehemiah Grew in his book, Philosophical Transactions. It was the first scientific reference to fingerprints, introduced in Argentina in 1891 by a Yugoslav, Juan Vucetich. Later in 1901, the British Police (Scotland Yard) became the first police force to adopt a system of fingerprint identification (Braggins, 2001). In recent years, iris scanning and facial recognition techniques have gained much interest. In the last decade, biometrics has grown significantly as large scale applications have started to unfold (Ashbourn, 1999).

Before discussing the different types of biometrics are available for identity checks and those that are suitable to be implemented at the airports, it is necessary to understand the physiological and behavioural characteristics that contribute to successful installation and authentication of passengers.

3.4.Characteristics of Biometrics

According to Vaclav and Zdenek (2000) and Prabhakar *et al.*. (2003), (cited in Zorkadis & Donos, 2004), any human physiological or behavioural characteristics can serve as biometrics whether for authentication or identification, if they fulfil the following properties:

- Universal – the biometric element exists in all people. In this respect, not all biometric elements are equivalent and the rate of distinguishing one person from another is very different, according to the type of biometrics used.
- Distinctiveness – the biometric element must be distinctive to each person, that is, no two persons should be the same in terms of the biometrics. Fingerprints have a high diversification and the probability of two persons to have the same iris is estimated as negligible. The most distinctive elements seem to be DNA, iris, retina and fingerprint.
- Permanence – the property of the biometric element remains invariant over time for each person. While some biometrics such as iris remains stable over decades, other biometrics such as a person's face or his signature's dynamics change over time. Also, fingers are frequently injured.
- Collectibility – the biometric characteristic should be quantitatively measurable and easy to collect. Retina scan and DNA analysis are quite intrusive, as opposed to face-related characteristics, which are easy to obtain.
- Performance – accuracy, speed, and resource requirements should be satisfied, in order for a biometrics-based system to be practical.
- Acceptability – indicates the extent to which a system is harmless and accepted by the intended users, in order to be of practical value.
- Circumvention – refers to the robustness of a system against various fraudulent methods and attacks, for instance against fake fingerprints.

Therefore, it is vital that a human being possesses the above mentioned characteristics for:

- Firstly, ensuring accurate identity verification and uniqueness of travellers; and,
- Secondly, to improve the performance of the biometric systems.

The next section presents the different types of biometrics that exist and those that are more suitable to be used at the airport.

3.5.Types of biometrics

Biometrics provide security benefits across many industry sectors. Different biometrics, however, may be appropriate for different applications and environmental conditions. Such biometrics, described in detail below, can be divided into two categories (Zorkadis & Donos, 2004):

- Physiological, and
- Behavioural.

3.5.1. Psychological

The psychological characteristics are used to verify an individual's identity. They consist of fingerprint verification, iris recognition, retina analysis, face recognition, ear shape recognition, and hand geometry

3.5.1.1. Fingerprint

A fingerprint is a pattern of ridges and valleys. According to Torbet *et al.*. (1995), the fingerprint is possibly the most commonly-known biometric, and its stability and uniqueness are well established. The first scientific

reference to fingerprints, as mentioned before, was in the 1684 case (Braggins, 2001).

Fingerprint identification has been used by detectives for more than a century to identify criminals. Automated fingerprint identification systems have been growing ever since the Federal Bureau of Investigation built the first computer-based system in 1967 (Sims, 1994). There are a variety of approaches to fingerprint verification. Some emulate the traditional police methods of matching minutiae; others use straight pattern-matching. Ridge endings and bifurcations together are referred as minutia (Ahmed & Siyal, 2005). While some can detect when a live finger is presented, some cannot (Liu & Silverman, 2001).

Due to its uniqueness with each individual, fingerprint biometric could be used both to allow travellers authentication, and let only authorized persons access restricted areas of the airport.

3.5.1.2. Hand Geometry

Hand geometry involves analyzing and measuring the shape of the hand. The biometric offers a good balance of performance characteristics and is relatively easy to use (Liu & Silverman, 2001). It might be suitable where there are more users or where users access the system infrequently and are perhaps less disciplined in their approach to the system (Liu & Silverman, 2001). Accuracy can be very high if desired, whilst flexible performance tuning and configuration can accommodate a wide range of applications.

Ease of integration into other systems and processes, coupled to ease of use makes hand geometry an obvious first step for many biometric projects (Ashbourn, 1999).

Hence, hand geometry could be well suited for identification of employee by monitoring their access to sensitive areas.

3.5.1.3. Face

Facial recognition has many practical applications in access control, security monitoring, and surveillance systems. Face recognition analyzes facial characteristics. It requires a digital camera to develop a facial image of the user for authentication (Liu & Silverman, 2001). The ability to recognize faces automatically with no conscious effort has probably made face recognition the most natural and popular biometrics (Zhang, Kundu, Goldgof, Sarkar & Tsap, 2004).

Human face recognition has been investigated before. Pentland and Choudhury (2000) state that twenty years ago, the problem of face recognition was considered among the most challenging in artificial intelligence and computer vision. Surprisingly, however, over the past decade, a series of advances have made general personal identification appear not only technically feasible but also economically practical.

However, as indicated by Campadelli, Lanzarotti and Savazzi (2003), face recognition remains an open problem; an effort is required to make the

existing techniques suitable for real applications, improving their computational performance and enlarging their field of applicability. Based on a large amount of research and benchmark studies, it has been recognized that visible photometric or geometric attributes present in intensity images for current face recognition methods suffer from problems associated with following factors (Zhang *et al.*, 2004):

- illumination and pose variation
- make-up, hairs and glasses
- plastic surgery
- face deformation during expression (dynamic face analysis in video sequence).

Thus more research needs to be conducted in the area of facial recognition to understand its suitability in the airport environment.

3.5.1.4. Retinal Scan

Retinal scanning analyzes the blood vessels in the back of the eye, utilizing a low density light source. While proven to be very accurate, it requires the subject to look directly into the scanning devise (Whisenant, 2003). According to Liu and Silverman (2001), retinal scanning can be quite accurate but not particular convenient if the users wear glasses or are concerned about having close contact with the reading devices. For these reasons, retinal scanning is not readily accepted by all users, even though the technology itself can work well (Liu & Silverman, 2001).

3.5.1.5. Iris

An iris scan analyzes the features within the coloured ring of tissue that surround the pupil (Whisenant, 2003). Compared with some other biometrics, such as fingerprints and face, iris recognition has had a relatively short history of use (Liu, Bowyer & Flynn, 2005).

Iris texture patterns are believed to be different for each person, and even for the two eyes of the same person. It is also claimed that for a given person, iris patterns change little after youth. Based on conceptual claims and empirical reports, the iris is often thought to be one of the highest accuracy biometrics because of its very high recognition or verification rates (Liu *et al.*, 2005). According to Whisenant (2003), the accuracy of iris scanning has an advantage over the retinal scan in its lack of intrusiveness. Also, a reading can be taken using conventional CCTV cameras which does not require the subject to come into physical contact with the equipment used to collect the sample (Whisenant, 2003).

3.5.1.6. Ear

According to Pun and Moon (2004), ears, although a newcomer in the biometrics field, have been long used as a means of human identification in the forensic field. Iannarelli reported, (cited in Pun & Moon, 2004), that ear growth after the first four months of birth is proportional to age. Moreover, according to Iannarelli, (cited in Yan & Bowyer, 2005), researchers have suggested that the shape and appearance of the human ear

is unique to each individual and relatively unchanging during the lifetime of an adult.

3.5.2. Behavioural

This measures the behaviour of a person, comprising of hand-written signature, and voice recognition.

3.5.2.1. Signature Verification

Signature verification analyzes the way a user signs his or her name. Signature features such as speed, velocity, and pressure are as important as the finished signature's static shape (Liu, 2001). The three likely advantages that signature verification presents over biometric techniques from the point of view of adoption in the market place are (Munich & Perona, 2003):

- It is a socially accepted identification.
- Most of the new generation of portable computers and personal digital assistants (PDAs) use handwriting as the main input channel. A signature may be changed by the user, similarly to a password, while it is not possible to change fingerprints, iris, or retina patterns.
- According to Munich and Perona (2003), for the identification of individuals in the many types of electronic transactions, automatic signature verification system has a unique possibility of becoming the accepted method for verification. Rhee, Cho, and Kim (2001) state that on-line signature verification is one of the most

applicable authentication methods in e-business, with applications in on-line banking transactions, electronic payments, access control, etc. However, according to Yamazaki, Mizutani and Komatsu (1999), the major problem associated with signature verification involves forgery handwriting because the same signature is used in both the enrolment and verification processes. There are three types of forgeries (Rhee, Cho & Kim, 2001):

I. Simple forgery – where the forger makes no attempt to stimulate or trace a genuine signature.
II. A random forger – in this type of forgery the forger uses his or her own signature instead of the signature to be tested.
III. A skilled forgery – in this category of forgery the forger tries and practices imitating it as closely as possible. A skilled forger may imitate the genuine signatures better than even the owner.

3.5.2.2. Voice Recognition

According to Vaughan-Nicholas (2004), voice authentication is becoming increasingly popular in the verification of individuals. Unlike other biometric approaches such a fingerprint or iris scans, a user can enrol in and work with a voice-authentication system from a remote location via a telephone (Vaughan-Nicholas, 2004). The advantages offered by voice biometrics over other authentication techniques are (Deshpande, Chikkerur & Govindaraju, 2005):

1) Usability;

2) Cost;

3) Ease of deployment; and

4) User acceptance.

Conversely, Shen pointed out, (cited in Vaughan-Nichols, 2004), the time required to verify a customer can be longer as voice templates are so much larger than other kinds of biometric information. Moreover, the accuracy of voice-authentication, in real world, is affected by changing factors such as background noise or changes in users' voice due to health, fatigue, or other causes (Vaughan-Nichols, 2004).

The above-mentioned physiological and behavioural characteristics of an individual are used to authenticate a user in a biometric system and to tighten security. The next section describes how the biometric system works and the processes involved in using the system.

3.6. The components of a Biometric System

As shown in the Figure 3: The Biometric Processes (Source: Kumar *et al.,* 2005), when a biometric is used to verify a person, the user first presents his or her biometric (for example, the thumb) to the sensor device, which captures it as raw biometric data (for example a fingerprint image).

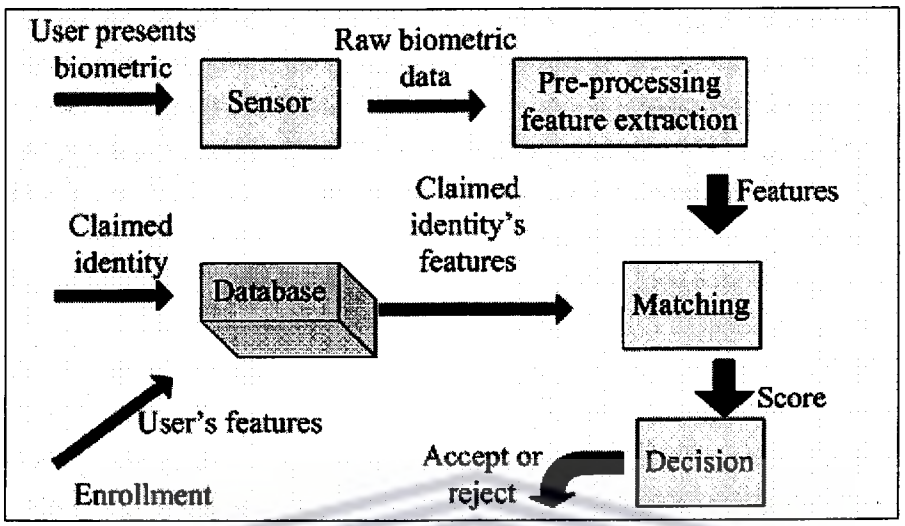


Figure 3: The Biometric Processes (Source: Kumar *et al.*, 2005)

This data is then pre-processed to reduce noise and enhance image contrast. features are then extracted from raw data. These features are then used to match against the corresponding user's features taken from the database (retrieved based on the claimed identity of the user). The final step is to compare the stored template with the live biometric. There are two possible outcomes (Kumar *et al.*, 2005):

1. Either the individual is rejected, if the template does not match; or
2. The individual is accepted, resulting from a matched template.

Thus, the step by step processes for authenticating an individual is (Liu & Silverman, 2001):

1. capture the chosen biometric;
2. process the biometric and extract and enrol the biometric template;
3. store the template in a local repository, a central repository, or a portable token such as smart card;
4. live-scan the chosen biometric;
5. process the biometric and extract the biometric template;

6. match the scanned biometric template against stored templates
7. provide a matching score to business applications;
8. record a secure audit trail with respect to system use.

The generated templates of one of the following, such as fingerprint, facial, iris, retina, hand geometry, and voice of individuals are used for either identification or verification in the automated biometrics-based system.

The following part shows the difference between identification and verification.

3.7. Distinguishing Between Identification and Verification

There are two distinct phases of operation for biometric systems namely, enrolment and verification or identification (Bennett, 2000).

Figure 4, below, illustrates a biometric system with two distinct phases:

1. Enrollment; and
2. Verification or identification.

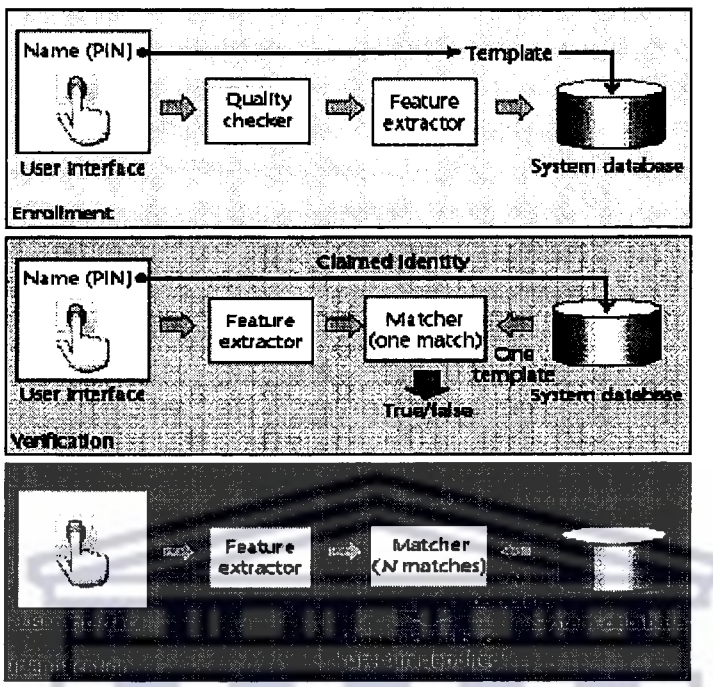


Figure 4: Verification and Identification (Source: Prabhakar *et al.*, 2003)

3.7.1. Enrollment

In the first phase, identity information from users is added to create the database that is used in the second phase, live biometric information from users is then compared with the stored records (Bennett, 2000). According to Jain *et al.*. (1999), (cited in Zorkadis & Donos, 2004), during the enrolment process, an input device specific to each type of biometrics is used to collect the biometric sample, the so-called biometric data (for example, image of the fingerprint, picture of the iris or of the retina, recording of the voice). This step of enrolment is then followed by either verification or identification for authenticating an individual.

3.7.2. Verification or Identification

A distinction needs to be made between:

- Verification, and
- Identification.

3.7.2.1. Verification:

Verification or one-to-one matching occurs when the user claims to be enrolled in the system by presenting an ID card or login name. The system compares the user's biometric data to the records in its database (Matyas & Riha, 2003).

3.7.2.2. Identification:

Identification also called search, recognition, or one-to-many matching, occurs when the user's identity is unknown. The system matches the user's biometric data against all records in the database as the user could be anywhere in the database or not there at all (Matyas & Riha, 2003).

For implementing an effective and efficient identification and verification system, proper security measures needs to be taken into consideration to assure the protection of enrolled biometrics template.

3.8. Factors necessary for an effective and efficient biometric system

For the designing and implementation of a biometric system, the key issues that need to be considered are:

- Reliability and robustness – It is important to consider how reliable the system is – in terms of continuing to perform at acceptable performance levels, and how robust the system is to fraud and impersonation. Such fraud can occur at the enrolment stage as well as at the verification stage. The system should ideally also be able to cope with small variations in biometrics over time (Bennett, 2000).

- Acceptability – This depends on the application and the location. The system must be easy to use, during both the enrolment and subsequent identification attempts. It must also be "acceptable". Users are often wary of systems that are perceived as invasions of privacy or confidentiality or perhaps systems that seem to view them as transgressors (breaking the rule) or potentially suspect (Bennett, 2000).
- Speed and storage requirements – the time required to complete the processes of enrolment and identification are very important in achieving acceptance of the system. Ideally, identification times should be of the order of one second or faster. The storage of templates is also an important issue – biometrics have large storage requirements; where storage is to be on a smart card, this may be critically important (Bennett, 2000).

3.9. Performance of the biometric system

There are different factors that need to be taken into consideration for biometric techniques to be successful.

According to Silverman *et al.* (2001), two factors can affect the conditions of biometric data:

- Time - Biometrics may change as an individual ages.
- Environmental conditions – These may either alter the biometric directly, for example, if a finger is cut or scarred, or interfere with data collection, for instance, background noise when using a voice biometric (Silverman *et al.*, 2001).

Other aspects identified by Torbet, Marshall, and Jones (1995) are:

- Speed of use, usability and customer acceptance;
- Device and card cost;
- Industry standards; and
- Recognition performance.

With regards to the latter, that is, recognition performance, two types of statistical errors can be caused by verifying the identity of an individual (Torbet *et al.*, 1995):

- Firstly, the device may reject a valid customer, and
- Secondly, the system may wrongly accept a fraudulent customer.

False Rejection Rate (FRR) and False Acceptance Rate (FAR) are used to evaluate the performance of the overall system (Wah & Feng, 2002).

3.9.1. False Acceptance Rate

FAR is the percentage of imposters incorrectly matched to a valid user's biometric (Silverman & Liu, 2001), that is, the biometric system gives access to an unauthorised user.

3.9.2. False Rejection Rate

FRR is the percentage of incorrectly rejected valid users (Silverman & Liu, 2001), that is, an authorized user being incorrectly rejected by the biometric system. According to Caelli *et al.*. (1994:514), false rejection can be caused by minor variations in the input. The variations that can arise each time a user try accessing the biometric system are (Caelli *et al.*, 1994:514):

- Environmental factors, such as temperature, background noise, and humidity, and;
- State of the user
    - Stress or perspiration
    - Wear and tear, for example the device being affected by dirt, grease, perspiration and minor injury.

Despite the potential benefits offered by biometrics, there are certain concerns that are raised by privacy advocates due to the fallibility of the technology.

3.12. Conclusion

This chapter has presented an overview of biometrics to introduce the different terminologies associated with this emerging technology. The different types of biometric technologies and their advantages has also been described, and showed how biometrics can be used in many applications to enhance the security measures by restricting unauthorised access. Furthermore, how a biometric system operates has been explained, as it involves registering and accurately identifying or verifying an individual in the automatic identification system.

The errors involved in the biometric system, such as FRR and FAR, have also been discussed. These errors may have an adverse effect on travellers, thus making individual reluctant to use these technologies despite the benefits being offered.

The next chapter will discuss, in more detail, the relationship in the literature between biometrics and privacy and show how some experts believe that biometrics can be privacy-enhancive and other believe that it can be privacy-invasive.

CHAPTER 4: BIOMETRICS AND PRIVACY

4. Introduction of privacy

In the previous chapter an overview of biometrics was given. This chapter presents the issue of privacy surrounding biometrics in the literature. The first part of the chapter focuses on the privacy concerns associated with biometric technologies and shows how informational and personal privacy can be jeopardized. Opposed to the first part, the next part gives an indication of the means by which biometrics could be used to enhance privacy. And finally, the last section represents how government regulations and information practices can be applied to improve security without compromising individuals' rights to privacy. Privacy is not a new issue; it can be tracked back many centuries.

4.1. History of privacy

Any organisation dealing with issues of security, authentication and identification will have many offers to solve problems through the use of a biometric system (Cavoukian, 1999b). Biometrics is believed to enhance the security in many applications. While the benefits of their use are quite tangible, there are also certain aspects in the use of biometric systems that raise concerns (Cavoukian, 1999b). One of these concerns is that of individual privacy (Cavoukian, 1999b). Privacy is a fundamental human right and has become one of the most important privileges of the modern age (Banisar, 2002). It underpins human dignity and other key values such as freedom of association and freedom of speech (Banisar, 2002).

As indicated by Arndt (2005) the underlying cause of privacy loss in the world in the second half of the twentieth century was an unprecedented growth in a wide range of technologies. The increasing sophistication of these information technologies facilitated the storage, processing and movement of information faster (Slemrod, 2006). This has allowed individuals to conduct their personal business with people and organisations that they do not know personally (Arndt, 2005).

In Europe, privacy concerns developed in the early 1970s as a result of growing information databases, and the use of personal identifiers to tag personal information (Kuzz & Colapinto, 2003). These databases consist of sensitive information stored after extensive data gathering, which can be accessed from anywhere in the country, thus giving rise to invasions of informational privacy (Graeff & Harmon, 2002).

Another issue related to the invasion of privacy is related to the identification of an individual. Several countries have witnessed public disquiet over identification schemes (Davis, 1994). These countries include Australia, Canada, the United States and New Zealand, where the community have concerns over identification schemes, and fear that (Davis, 1994):

- people will be de-humanized by being reduced to codes;
- the system will enhance the power over individuals of particular organisations and the state;
- high-integrity identification embodies an inversion of the appropriate relationship between the citizen and the state; and,
- the system is a hostile symbol of authority.

Thus, there is no doubt that privacy concerns raised by technologies for the extensive data gathering among individuals are significant. As indicated by Graeff and Harmon (2002), reasons for collecting data have been driven in large by the competitive forces facing marketers today.

The following section presents a definition of the separated, but related, concept of privacy. Different people ascribe different meanings and values to privacy violation that is now greater than at any time in recent history.

4.2. Privacy definition

It is important to understand what privacy really is and why there is a sudden interest in privacy issues related to the deployment of biometrics. Michael, (cited in Banisar, 2002), states that of all the human rights in the international catalogue, privacy is perhaps the most difficult to define. In addition the Privacy and Human Rights lobby has a similar view about privacy (Ayoade & Kosuge, 2002).

Below is a list of definitions of privacy according to different authors:

- In 1890, Brandeis and Warren defined the right to privacy as "the right to be let alone" (Loring (2002).
- Westin, (cited in Koneya, 1977), defines privacy as the right that individuals have to control what information about themselves should or should not be communicated to others and under what conditions.
- Privacy is often thought of as a moral or legal right. But it's often more useful to perceive it as the interest that individuals have in sustaining a personal space, free from interference by other people and organisations (Clarke, 1999).

- According to Prabhakar, Pankanti, and Jain (2003), privacy is the ability to lead a life free of intrusions, to remain autonomous; and the ability for an individual to control access to personal information.

Despite all the different definitions from different authors, according to Banisar (2002) privacy can be divided into the following separate, but related concepts:

- Information privacy, which involves the establishment of rules governing the collection and handling of personal data such as credit information, and medical and government records. It is also known as "data protection";
- Bodily privacy, which concerns the protection of people's physical selves against invasive procedures such as unsolicited genetic tests, drug testing and cavity searches;
- Privacy of communications, which covers the security and privacy of mail, telephones, e-mail and other forms of communication; and
- Territorial privacy, which concerns the setting of limits on intrusion into the domestic and other environments such as the workplace or public space. This includes searches, video surveillance and ID checks.

Of all the above-mentioned privacy, informational privacy is creating most of the controversy today, as personal information is being collected and used by businesses day-in and day-out to gain competitive advantage.

For this research project the focus will be on informational privacy. With respect to the latter, there are at least two important ways in which the introduction of new technologies, such as biometrics, can raise privacy concerns (Tavani, 1999):

- Firstly, the technology can be used to collect information about an individual or group of individuals without their awareness or knowledge; and
- Secondly, individuals are aware that information about them is being collected via a certain technology, but have no say in how the information about them is to be used (disclosed, exchanged, sold, etc).

From the above, it is evident that emerging technologies are creating privacy fears. As discussed below in more detail, biometrics, which are used to authenticate individuals by capturing the behavioural and physical characteristics, despite offering enhanced security, also raise privacy concerns.

4.3. Biometrics and Privacy

Civil liberties groups have shown concerns about the extensive adoption of the biometric technologies and believe that biometrics give rise to privacy concerns. The questions that need to be asked about biometrics, in this regard, are:

1. What is it that gives rise to privacy concerns, or threatens individuals' rights to privacy?
2. How do people's privacy attitudes affect the acceptance of biometric technologies?
3. What are the different aspects or factors that endanger privacy rights?

4.3.1. What Gives Rise to Privacy Concerns?

With respect to the first question, Langenderfer and Linnhoff (2005) state that it is the swift growth of biometrics that has spurred a concomitant concern among many special interest groups and consumers regarding the privacy and effectiveness of the system. The rapid progress of biometric technologies and their expanded use in the public sector, in the workplace, and at home are raising specific concerns from a legal point of view; especially the legislation concerning privacy and personal data protection (Zorkadis, Donos, 2004).

4.3.2. People Privacy Attitude

Regarding the second question, research has shown that attitudes towards privacy are an important factor when considering the acceptance of biometrics (Paine, Joinson, Buchanan & Reips, 2005). The three categories of respondents are (Paine *et al.*, 2005):

- **The privacy fundamentalists**

  The privacy fundamentalists view privacy as an especially high value which they feel very strongly about and they usually have high levels of distrust. They tend to feel that they have lost a lot of their privacy and are strongly resistant to any further erosion of it.

- **The privacy pragmatists**

  Privacy pragmatists also have strong feelings about privacy and tend to have medium to high levels of distrust. They are very concerned to protect themselves from misuse of their personal information by other people and organisations. They weigh the value to them and society of providing personal information, and are

often willing to allow people to have access to, and to use, their personal information – where they understand the reasons for its use, can see the benefits for so doing and when they believe care is taken to prevent the misuse of this information.

- **The privacy unconcerned**

The privacy unconcerned have no real concerns about privacy or about how other people and organisations are using information about them. They usually have low to no levels of distrust.

Public privacy attitudes are subjective (Paine *et al.*, 2005), and regarded as an important factor towards the acceptance of biometrics. As a result the levels of privacy attitudes will undoubtedly vary from person to person based on individual perceptions and values.

4.3.3. Factors endangering privacy rights

Lastly, this section replies to question three which explains the different factors that raise privacy concerns. More than thirty human rights and civil liberty organisations worldwide have expressed mounting concern to the International Civil Aviation Organisation (ICAO)[2] regarding the use of biometrics in travel documents and they feel that these technologies are still emerging and clearly fallible (Most, 2004). Since the use of biometrics for identification has the potential to be imperfect and privacy

[2] ICAO works to achieve its vision of safe, secure and sustainable development of civil aviation through cooperation amongst its member states. Available at: http://www.icao.int/icao/en/strategic_objectives.htm

invasive it is highly probable that problems will arise through the use of a biometric system.

As stated by Jain, Hong and Pankanti (2000) the overall performance of a biometric system is assessed in terms of its accuracy, speed, and storage. When identification is necessary, it is important to ensure the system is authoritative, accurate and fraud-resistant (Mladen, 2002).

The remaining factors raising privacy concerns (from the points given above), among civil liberties group with regards to biometrics' systems are:

4. Function creep; and
5. Identity theft.

For this research, the privacy-related concern is mainly centred on informational privacy. Accordingly, it is important to discuss how the above-mentioned factors impact on informational privacy.

4.3.3.1. Accuracy of the biometric systems

Biometric systems do not provide absolute accuracy, and are not perfect. Alterman (2003) suggests that the problems with the former are the False Acceptance Rate (FAR) and False Rejection Rate (FRR). Biometric systems will sometimes mistakenly accept an impostor as a valid individual or conversely, reject a valid individual (Jain, Hong & Pankanti, 2000), even though the magnitudes of these errors depend upon how liberally or conservatively the biometric system operates (Jain, Hong & Pankanti, 2000). It is generally agreed that fingerprint technology is the most reliable of all

biometric technologies despite vendors claiming a FAR and FRR of 0.01% or less, meaning that less than one in 10000 people are matched with someone else's fingerprint (FAR) or fail to be matched with their own fingerprint (FRR). As a result, the collection, storage, and use of personal biometrics data pose a serious threat to informational privacy as it is believed that personal data can be stolen or modified to get access to the system by an imposter. Another problem with informational privacy is the storage of biometric data in a database.

4.3.3.2. Database

As claimed by Most (2004) the most significant informational privacy concerns and invasion of privacy is the storage of sensitive biometric data in a centralized database. This is a result of today's technology that allows more extensive gathering of sensitive data during enrolment of individuals (Graeff & Harmon, 2002). As a consequence, the easy accessibility of such databases from anywhere in a country has raised fears among civil liberty groups (Scherer, 2005). People worry that their every move could be tracked and monitored on an ongoing basis. Also, as indicated by Roger (2005), if these databases fall into the wrong hands, they could then be misused and made available to government agencies and business entities by the many security, law-enforcement, border-control, medical, and banking organisations that maintain vast biometric databases, thus resulting in the abuses in personal freedom and privacy (Scherer, 2005). In addition, these databases can be merged to provide an in-depth portrait of an individual's behaviour (Graeff & Harmon, 2002).

The informational privacy concern is related to "Function Creep" as well.

4.3.3.3.Function Creep

As pointed out by Langenderfer and Linnhoff (2005), function creep refers to the dangers of finding biometric data exchanged without consent, within the biometric community. Function creep has the potential to undermine data protection features, as it will spread bearer data more widely across divergent systems (Juels, Molnar, Wagner, 2005).

Function creep problems may lead to biometrics giving away DNA, racial or health information about the enrolee that he or she may wish to keep private, be used for commercial purposes, or even for tracking and surveillance (Thomas, 2005). The problem of function creep has already come to light with the occurrence and advanced passenger screening programmes, undertaken in Australia, Canada, the US and the UK (Thomas, 2005).

Adey (2004) indicates that biometric systems are of obvious concern to proponents of privacy, as the stored data has the possibility to be hacked, shared and misused by external sources or third party, resulting in the increasing trouble in the invasion of privacy and the possibilities for expansive data share.

A different concern related to informational privacy is identity theft.

4.3.3.4. Identity theft

Undoubtedly the greatest concern among people is the theft of their personal information. Identity theft is the act of obtaining personal information without the concerned person's consent (Friedewald, Vildjiounaite, Punie and Wright, 2006). The

more widely personal information becomes available, the greater is the risk of it being stolen by malicious persons and being used for fraud and other illegal activities (Friedewald *et al.*, 2006).

The increasing growth in identity theft of non-revocable biometric templates has alerted the public to the privacy issue (Connie, Teoh, Goh and Ngo, 2004). A biometric template once compromised is rendered unusable. This is exacerbated by the fact that a new template cannot be assigned (Connie *et al.*, 2004). The only remedy is to replace the template with another biometric feature, taking into account that a person has only limited number of biometric features that can be used (Connie *et al.*, 2004). So, people are rightfully concerned about their identity being used for fraudulent transactions by impostors.

In summary, informational privacy concerns described by Moore (2003) are the unauthorised collection, use, retention, and disclosure of biometric data which are described below.

4.3.3.5. Unauthorised Collection

It allows for the population of biometric databases and execution of biometric matches without users consent or awareness.

4.3.3.6. Unauthorised use

This encompasses methods by which biometric data can be used for purposes broader than those originally intended, including use in tracking, conducting searches against commercial or government databases.

4.3.3.7. Unauthorised retention

The unauthorised retention of biometric data, in which biometric information is stored longer than necessary, is of concern in certain biometric systems. If information originally intended to be deleted is instead retained, the ability to perform various types of operations is also retained.

4.3.3.8. Unauthorised disclosure

Unauthorised disclosure of biometric information to other public agencies or to private sector institutions undermines an individual's control over his or her own personal data. Unauthorised disclosure increases the likelihood that biometric data will be used for purposes beyond which it was originally intended.

The above concerns are rooted in the fundamental privacy concept that individuals have a right to control access to and usage of their personal data.

As opposed to the above section that shows that biometrics give rise to informational privacy, the next part will explain how proper safeguards can make biometrics more privacy-enhancing.

4.4. Privacy-enhancing biometrics system

Even though biometrics threaten the individual's right to privacy; it is also regarded as privacy-enhancing. The question that needs to be considered is how can privacy rights and civil liberties of individuals not only be maintained but be directly enhanced by the widespread deployment of biometrics (Most, 2004).

As stated by Wright (2005), despite biometrics being the technology that raise concerns about the security of the stored data against which biometric matches are made, it is also one of the potentially privacy-enhancing technologies. Supporting this claim is Taipale (2004/2005) who states that identification systems can enhance privacy when they are used to secure data or to protect identity, for example, by ensuring that an individual is indeed the authorised user of a credit card or a particular computer, or is permitted access to certain information. As listed below, biometric systems which are considered as privacy-enhancing among privacy opponents can be used in different situations for higher security.

4.4.3. Combat fraud

Firstly, fraud and breaches of security are of great concern in the banking industry and are thus considered to be a significant problem (Cavoukian, 1999a). Davis (1999) mentioned that biometrics is increasingly seen as a solution to fraud and inefficiency, in particular finger scanning (Cavoukian, 1999a). Various nations around the world are adopting biometric technologies to assist in such activities as recording population growth, identifying citizens and preventing fraud in elections (Cavoukian, 1999b). Moreover, as Cavoukian (1999b), continues biometrics can also be used in airports to improve security. Thus, an increase of awareness in the use of biometrics among individuals can help in the adoption of the technologies in different application and combating fraud. According to Giesing (2003), a lack of information would prevent users from making use of a biometric identification system because they do not realize what it is capable of.

4.4.4. Biometric Data Protection

Secondly, in a privacy-enhancing biometric system security measures must be taken when biometric data is processed. Loring (2002) indicates that the notion of protecting of personal data and privacy of individual citizens is a fundamental right, thus preventative measures must be undertaken in order to avoid abuses of privacy.

Data Protection, a European term closely associated with informational privacy, refers to policies designated to regulate the collection, storage, use, or dissemination of personal information (Loring, 2002). The Data protection act was first passed in Sweden in 1973, soon followed by Germany, Denmark, Norway and France. In 1995 the European Union issued a directive to its member states requiring them to bring their national data protection laws into compliance (Kuzz, Colapinto, 2003). Moreover, as mentioned by Dumortier and Kindt (2005), any person acting under the authority of the controller or of the processor, including the processor himself, who has access to personal data, must not process them except on instructions from the controller, unless he is required to do so by law.

Thus, privacy violations can be prevented during all stages of data processing; such as unlawful storage or storage of inaccurate personal data or the abuse or unauthorised disclosure of personal data if proper privacy protections are put in place (Zorkadis & Donos, 2004).

4.4.5. Encryption

Thirdly, decrypted biometric templates can be defenceless in an attack. Therefore, an important way of safeguarding privacy and identity of individuals is by encrypting the

stored biometric data (Wright, 2005). Reliable forms of encryption can anonymize data and prevent unauthorised third parties from intercepting confidential information (Cavoukian, 1999a). Encryption of the templates during biometrics data process such as storage, transmission, extraction of characteristics and comparison could instead results in a perfect privacy-friendly biometric system (Zorkadis & Donos, 2004).

Also, decentralisation of the biometric template can be a possible solution to minimise the privacy risk.

4.4.6. Decentralisation

Fourthly, biometric data can be protected and controlled by the bearer of the information if it is stored in a decentralised system. One way to decentralize a biometric system is to store the biometric information not in a centralized server but in decentralised, encrypted databases, over which the individual has complete control (Prabhakar *et al.*, 2003). For instance, a system could issue the user a smart card with his or her biometric information stored as a template on it (Prabhakar *et al.*, 2003). Such a decentralised system would permit all the advantages of biometric-based recognition without many of its stipulated privacy problems (Prabhakar *et al.*, 2003). Storing an individual's biometrics on a personal device such as smart card is the least invasive way of verification (Most, 2004).

Some manufacturers are relying on smart cards to control access which encode fingerprint data in the smart card's microprocessor so it operates like a bank cash machine where one enters the card and a personal identification number (PIN)

(Desmarais, 2000). As a result, there is no need to have a massive centralized database in order to confirm the identity of an individual.

In the above section we have seen how the widespread use of biometrics and certain factors can enhance privacy rights and not violate them. The next section revolves around how privacy concerns can be balanced with the benefits of biometrics to help convince individuals to present their biometric data to an organisation for a specific purpose and not for their detriment.

4.5. Balancing Privacy and Security

If proper privacy safeguards are built into the biometric systems, they would prove useful in dealing with troublesome privacy proponents. As mentioned below, security of data and information practices can help break the conundrum between privacy and security of biometric usage among travellers in the airport and protect biometric data without compromising privacy.

The first factor that needs consideration regarding sensitive biometric data is the personnel in charge of the sensitive information. Zorkadis and Donos (2004) suggest that the data controller must take all appropriate technical and organisational security measures when biometrics data are processed during storage, transmission, extraction of characteristic, and comparison in order to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access.

Secondly, data security is one of the most important parts of privacy protection legislation (Zorkadis & Donos, 2004). Udo (2001) defines security of biometrics as the protection of data against accidental or intentional disclosure to unauthorised modifications or destruction. Ponemon, CEO of PrivacyCouncil, believes that security can be improved without compromising privacy (Sanborn *et al.*, 2001) by doing the following:

1. Determine and share an individual's risk status information with other companies, but share on a need-to-know basis. All other sharing of such information should require the consent of the individual.
2. Maintain high security standards around the clock. If security data gets into the wrong hands, it could be used to discriminate, or worse.
3. In tracking suspicious activity, ensure there are clear reporting channels so that information gets into the right hands.
4. If surveillance is misused, have enforcement and a means of redress in place; organisations that do not respect the proper use of surveillance and misuse the data should face fierce penalties.
5. Set up some form of independent checks and balance to make sure surveillance is appropriate.

Finally, information practices can help overcome the problem of privacy regarding biometrics information. The Federal Trade Commission (FTC) (1998), (cited in Langenderfer & Linhoff, 2005), indicate that more than 30 years ago, the US Department of Health, Education, and Welfare issued a report articulating a list of "fair information practice principles" that have become the *de facto* standard for

assessing the privacy protection appropriateness of various information practices. The principles are as follows (Langenderfer & Linhoff, 2005):

1. Notice/awareness – No data should be collected from individuals that they are not aware is being collected.
2. Choice/consent – Individuals should have a choice as to how their information is used and distributed.
3. Access/participation – Individuals should have the right to view any data files about them and the right to contest the completeness and accuracy of those files.
4. Integrity/security – Organisations in the business of data collection must take steps to ensure that the data are accurate and secure from unauthorised access.
5. Enforcement/redress – Individuals must have an avenue of redress for violations of the above principles, with an enforcement mechanism to ensure compliance.

In summary, the general advantages of biometrics authentication while simultaneously protecting people's privacy as compared to the traditional methods of authentication such as pin codes, passwords, electronic signature or encryption keys in the recognition of an individual are (Grijpink, 2001):

1. Biometrics template should always be carried with the individual and not left at home.
2. The biometric characteristic should not be transferred to someone else unobtrusively.
3. A detached biometric characteristic should not be traced back to the person from whom it originated without additional clues.

4. Biometrics techniques should not be subjected to recognition errors that could result from faulty observation such as preconceptions, distraction or tiredness.

4.6. Conclusion

In this information technology era, the issue of privacy and security is high on every individual's agenda. To improve security and authenticate consumers, there appears to be an increase in the use of biometrics in different applications. At the same time, there is an increase in privacy concerns related to biometrics.

In the first part of this chapter the definition and history of privacy in the literature was discussed. Then the relationship that exists between biometric and privacy were explained.

Firstly, privacy-invasive issues related to biometrics were described, indicating why individuals are reluctant or against the use of biometrics. Factors that were identified that give rise to privacy concerns were the unauthorised use, central data storage, error related to authentication (FAR and FRR), and improper access to an individual's personal biometric information.

Conversely, the next section showed that there are people who believe that biometrics can be more reliable than any other methods of authentication and can enhance privacy. Encryption, decentralisation of the template, and data protection are considered appropriate methods to meet the requirements for a privacy enhancing biometric system.

And, finally, it is believed that privacy and biometrics can co-exist if new information practices are incorporated into the biometric systems thus protecting individual biometrics information.

Described in the next chapter is the research methodology and the steps required to design a reliable survey questionnaire.

CHAPTER 5: RESEARCH METHODOLOGY

5.1.Introduction

This chapter focuses on the design, formatting and administration of a survey questionnaire. First of all, this chapter provides an understanding of the research methodology used for this research. It is a combination of quantitative and qualitative approaches. The qualitative research, which involved the use of qualitative data from published articles, was used to understand the social occurrence in greater detail, and to identify the items for the questionnaire. On the other hand, a quantitative methodology was suitable at summarising the large amount of data collected through the questionnaires and to test the hypotheses between the variables.

Secondly, McClelland (1994) states that, choosing the proper structure for a questionnaire is a critical factor in determining and ultimately obtaining unbiased feedback. Since a self-administered questionnaire given to a sample of travellers was considered appropriate, several factors were taken into consideration in designing the instrument that investigated respondent perceptions. For a reliability and validity check, the survey instrument was pre-tested to highlight mistakes, problems or oversights.

5.2.Research Methods

Research approaches can be categorised into two common methodologies: qualitative and quantitative methods. The distinction between the two includes the following:

- Qualitative methods are useful in the exploratory stages of a research project, where they can help to clarify or set the research question, aid

conceptualisation and generate hypotheses for later research. They may also be used to interpret, qualify or illuminate findings of quantitative research and to test hypotheses (Elizabeth, 2000).

- In the social sciences, quantitative research is often contrasted with qualitative research, which is the examination, analysis and interpretation of observations for the purpose of discovering underlying meanings and patterns of relationships, including classification of types of phenomena and entities. Statistics is the most widely used branch of mathematics in quantitative research (Wikipedia, 2006).

However, as claimed by Moore, (cited in Williams & Gunter, 2006), it is extremely fruitful to combine quantitative and qualitative data to interpret user behaviour, as quantitative data is very good at telling what is happening, while qualitative provides an insight into the deeper question "*why*?". Hence, this research being a combination of the two. Although qualitative research was necessary to generate theories and identify relevant variables for the hypotheses, quantitative research involved the collection and analysis of numerical data through the use of a survey questionnaire.

5.3.Research instrument

For the purpose of this research, a survey questionnaire was considered a useful tool to gather primary data from travellers. It is important to develop a survey instrument unique to this research because of the several areas it deals with. Survey methodology is popular for a number of reasons (Chauvel & Despres, 2002):

1. First, it brings an issue into focus by defining and detailing its various characteristics, which, in a reporting phase, causes users to focus their attention.
2. Second, the results of a survey are typically quantified and therefore amenable to statistical treatment.
3. Third, statistical inference allows an extention of the results obtained from a sample of respondents to a larger population, thereby permitting a more global statement.
4. Fourth, it cannot be ignored that survey methodology is fast and straightforward compared to many other research methods.

A similar view is shared by McClelland (1994). He indicates that the advantages in using a questionnaire to gather data are:

1. Firstly, they can be administered to a large population.
2. Secondly, they are non-intrusive means for gathering feedback, as opposed to individual interviews, focus groups, and sometimes on-site observations, because respondents can provide input in a tension or intimidation-free environment and at their convenience.
3. Thirdly, bias, which can easily surface in individual interviews owing to the manner in which questions are posed by the interviewer and are perceived by the respondent, is minimised.
4. And finally, completing questionnaires is relatively simple and straightforward and does not require an excessive amount of time.

However, it is important to take special care in designing an appropriate questionnaire. The questionnaire items were generated from a thorough analysis of the literature as discussed in the previous chapters. It was piloted and refined through several versions. Once the design of the questionnaire was completed, it was administered to 150 respondents.

5.4.Questionnaire Design

As indicated by Janes (1999), in order to encourage people to complete the survey it is important to make the survey as easy, fun, interesting and worthwhile as possible. Moreover, as suggested by Veal (cited in Kivela, Reece, Inbakaran, 1999), it is desirable to develop a research instrument that operationalises the research questions and research objectives, and the theoretical model.

As shown in Figure 5: Survey instrument break-down (below), in order to gather data, the survey questionnaire was divided into two sections: the demographic section and the main body.

Section	Contents	Structure
[redacted]	•Surname •Address •Gender •Age •Occupation •How often do you travel every year	Closed-end answers
[redacted]	•General Security •Acceptance of Biometrics •Privacy invasive technology •Privacy Protection •Balance between privacy and security	6-point Likert scale and "statement not relevant" option
	•Check-in procedure •Data collection •Data storage	

Figure 5: Survey instrument break-down

The first section of the survey instrument contains demographic information, such as surname, address, age group, gender, air travel frequency and purpose of travel to respondents. The second section of the questionnaire consists of 27 items using a 6-point Likert scale ranging from "Totally disagree" to "Totally agree" that explore each of the different dimensions, namely: General Security, Acceptance of Biometrics, Privacy, Protecting Biometric Information, and Balancing Security and Privacy. Additional provision was made for a respondent to select a "statement not relevant" option. Three more items were added relating to:

- The check-in procedure at airport,
- The personal data storage, and
- Personal data collection.

The abovementioned items measure and give a better understanding of the privacy-related issue regarding the use of biometrics. After the items were gathered, respondents were asked to express their degree of agreement and disagree using a 6-point Likert scale. The Likert technique is presented in greater detail below.

5.5.Likert Scale

Lin (1976:183) suggests that the best-known summated scale in social research is probably the type initially proposed by Likert to measure respondents' attitude toward certain issues. The use of a Likert scale involves the following procedure (Lin, 1976:183):

1. Initial construction and selection of positive and negative statements about an issue with response categories for each statement,
2. Collection of responses to these statements from a group of respondents,
3. Computation of total scores for the respondents across all statements,
4. Examination of the consistency of the response pattern for each statement relative to the total scores received,
5. Elimination of inconsistent statements,
6. Compilation of the final set of statements, and
7. Recomputation of total scores for the respondents based on this final set.

These questions or statements require respondents to select their most suitable answer from a 6- or 7-point scale so that their various levels of expectation can be distinguished more clearly. As mentioned by Mansfield (2005), there is evidence that 6- to 7- point scales are optimal, especially if several different instruments are employed concurrently. Also, the 6-point Likert is considered appropriate as it tends

to avoid the 'neutral' central tendency. According to De Vaus (cited in McMullan, 2005) one of the main values of a scale is its ability to measure a concept by using multiple indicators rather than one, which facilitate tapping the complexity of concepts. The neutral point of the Likert scale has been shown to not significantly affect an individual's composite score (Mansfield, 2005).

Accordingly, the instrument in this study was administered in the form of a 6-point Likert scale, with additional provision made for a respondent to select a "statement not relevant" option, similar to the one used by Mansfield (2005) in his research. Thus, the order of the degrees of agreement or disagreement on the questionnaire (see Figure 6: Likert Scale) for each question was as follows (Smith, 1972:79):

Degree of Disagreement	Degree of Agreement	Option Statement
Totally disagree	Sometimes agree	Statement not relevant
Mostly disagree	Mostly agree	
Sometimes disagree	Totally agree	

Figure 6: Likert Scale

The statements were listed on the questionnaire with seven columns, as shown in figure 7, each headed with one of these expressions denoting degrees of agreement and disagreement and "statement not relevant" arranged beside them.

	Totally Disagree (1)	Mostly Disagree (2)	Sometimes Disagree (3)	Sometimes Agree (4)	Mostly Agree (5)	Totally Agree (6)	Statement not relevant
Item							
Q1							

Figure 7: Likert Scale Format on Questionnaire

The first section collected demographic information of travellers in Cape Town so that a comparison could be made between the different groups of individuals, such as gender, age and education.

Once the items of the questionnaire were identified, it was important to take those factors into consideration that may produce biased results, and avoid them.

5.6.Minimising Bias

Firstly, in order to avoid bias, the data collection part of the survey (carried out at the airport) focused on air passengers. Secondly, the order of the items on the questionnaire might influence individuals' perceptions. The general order of the questions makes some difference. Therefore, the questionnaire was organised so that one question flowed from another (Weisberg & Bowen, 1977). Lastly, to avoid response biases, half of the items were stated in the negative direction, with the others in the positive direction. As Lin (1976:184) indicates, for a summated scale it is desirable to contain positive and negative statements in equal numbers and presented at random. Once instrument bias has been avoided, it is important to have a reliability and validity check so that the questions in the questionnaire focus directly on the specific issue and provide brevity and clarity.

5.7.Reliability and Validity check

According to Mansfield (2005), there is a difference between validity and reliability. Validity refers to whether an instrument measures what it is designed to measure whereas the instrument is said to be reliable if repeated measurements, made on the same object, are stable.

In order to evaluate the validity of the questionnaire, a pilot test was conducted with 10 randomly selected respondents. In addition, it was also evaluated by a group of experts to solicit comments and suggestions about the instrument, and to assess the duration of a survey questionnaire in order to estimate the average time for completing the questionnaire. According to Judd, Smith, and Kidder (cited in Yang, Jun, Peterson, 2004), content validity can be evaluated by a group of judges, sometimes experts, who read or look at a measuring techniques and decide whether in their opinion it measures what its name suggests.

As for the reliability test, Cronbach's α coefficient is the most frequently used indicator of instruments in survey research (Kivela *et al.*, 1999). Another way of testing the reliability of data obtained is indicated by Smith (1972:25) in her book, "Interviewing in the market and social research". According to Smith, in order to check that data obtained from personal interviews are reliable, the same questions will be asked of the same respondent by different interviewers and the results compared. Finally, to enhance the reliability and validity, great care must be taken while designing the questionnaire.

After the reliability and validity check, the last step in questionnaire design is to test the questionnaire, as discussed below.

5.8.Pre-test and pilot test

As McClelland (1994) indicated, a draft questionnaire should be subjected to a pre-test in which it is proofread for typographical errors, vague and/or misleading

statements, and neutral phrasing as it serves to establish the framework for validity and reliability. Once the questionnaire was tested, proofread and finalized, it was pilot tested by a group of travellers. If respondents do not show any major problems with the questionnaire, the survey would be conducted. However, if travellers experienced problems completing the questionnaire, it would be re-edited and retested. After a successful pilot test, the questionnaires were used to collect data through proper research methods, as discussed in the next section.

Before the questionnaires were distributed, it was important to identify the target population of the study in order to avoid bias. The next section will discuss the sampling technique or method and the sample design.

5.9.Sample Design and Sample Technique

To administer the questionnaire for this research, a systematic selection of 150 respondents was considered appropriate, that would provide a meaningful representation of the sample group. The sampling frame included respondents located in the City of Cape Town and who are 18 years of age, or older.

Travellers were selected by a systematic sampling method to avoid bias. Systematic sampling is a widely used technique in which, to obtain a sample of n subjects from a list on N potential subjects, one selects every i^{th} subject (where $i = N/n$), after a random start (Elliott, Nerney, Jones & Friedmann, 2002). For this research, every 2^{nd} (i^{th}) traveller was chosen. Once the target sample is identified it is important to decide on the research method or data collection method.

5.10. Research method

A survey is a good way, often the only way, of getting a picture of the current state of (Janes, 1999):

1. A group,
2. A community,
3. An organisation,
4. An electorate,
5. A set of corporations, and
6. A profession.

Hence, to conduct this survey, a suitable research method had to be selected. As stated by Stephen (1995), research methods are concerned with investigation and data collection. Thus, to gather primary data, the research methods for this survey included self-administered questionnaires, that is, mail and handout. As Stephen (1995) indicates, the techniques employed to collect data should give an adequate and true picture of the topic of investigation, and provide controls to try to ensure that data are as free as possible from bias and irrelevance.

5.11. Data Analysis (editing and coding)

As indicated by Janes (1999), once the data has been gathered it is important to perform the appropriate kinds of analysis to tell the world what the data means: what the answers to the research questions mean in the grander scheme of things, and how it might make a difference. First of all, it is important to code the Likert scale (data) in order to analyse the data meaningfully. Each point on the 6-point Likert scale, which expresses travellers' perceived level of agreement or disagreement of the security and

privacy issues of biometrics at airports, was assigned with a number with the score ranging from:

1 = "Totally disagree"	4 = "Sometimes agree"
2 = "Mostly disagree"	5 = "Mostly agree"
3 = "Sometimes disagree"	6 = "Totally agree"

For each item, half of the Likert scale with the opinion "disagree" signifies a negative attitude and the remaining half with the opinion "agree" signify a positive attitude.

The next step was to analyse the data by importing it into the SPSS statistical program, version 11. Descriptive statistics processes were applied. Descriptive statistics provide basic information such as the mean, minimum and maximum values, different measures of variation, as well as data about the shape of the distribution of the variable (Mansfield, 2005). Measures of variation include the standard deviation and the standard error (Mansfield, 2005).

Statistical tests are considered appropriate, providing that the data have been collected properly, as they are neutral and unemotional (Stephen & Hornby, 1995). Statistical software packages, such as SPSS are used, since they are "ruthlessly logical" (Stephen & Hornby, 1995).

The data was analysed at the Statistics Department of the University of the Western Cape. Data analysis is discussed in detail in the chapter 6.

Missing values could be caused by a number of factors. For example respondents may complete most of the questionnaire but not answer some questions due to exhaustion or fatigue. Missing values are discussed in the section that follows.

5.12. Missing Data

Missing data imputation has become the norm in larger data collection efforts. Its benefits are starting to have an impact on organisational research (Chen & Astebro, 2003). In this research, questionnaires with more than six missing items, which represents 20% of the overall items, were excluded. Missing data and answers in the "Statement not relevant" category were substituted with the average score of the corresponding dimension.

5.13. Construct Operationalisation

In this section, the operationalisation of the research construct, the measures and items, and their origin in literature are summarised in the different tables mentioned in the different sub-sections that follows below. The design of the questionnaire was based on five dimensions. Each dimension was mentioned in detail in the previous chapter. However, a brief summary of each dimension is described below. The questionnaire items have their origins in the earlier discussion.

5.13.1. General Security

There is a need to improve the security of airports, for example verifying the identity of passengers, flight crew members, and employee identity so that travellers are safe. Baggage handling must be taken into consideration as well. Also, there is a necessity to control access to sensitive areas within the airport. **Error! Reference source not**

found.) shows the different questions that were generated and used to measure the travellers' concerns, such as terrorism and personal rights, and experiences of current security, for example, passengers' screeners at the airport.

General Security		
Measure	Source	Questionnaire Item
Threat of terrorists	Lewis, Curt, Montgomery and John (1989)	There is a serious threat that airport terrorist attacks that have occurred in the past, could happen again.
Protecting Passengers	Coughlin, Cohen and Khan (2002)	The airline industry is liable (has a legal responsibility) for protecting passengers from terrorist attacks.
Screen staff	Postnote (2001)	All airline and airport personnel should be screened to ensure they have no criminal record.
Secure from hostile individuals	Babu, Batta and Lin (2006)	I have full confidence in the ability of the passenger screeners to keep air travel secure from hostile individuals.
Effectiveness of staff	Turney *et al.* (2004)	Security staff using X-rays screen hand-luggage effectively.
Safety or personal rights	Stibb (2005)	I am more concerned about safety than my personal rights – for example, I do not object to being searched.

Table 2: General security section: Questionnaire

5.13.2. Acceptance of Biometrics

The identity of an individual is authenticated by either something he or she knows. For the traveller, it would be things such as a passport, or something the passenger (individual) actually is, such as biometrics. As discussed in detail in chapter 3, biometrics technology is considered as the most secure form of authentication to verify individuals, based on their unique biological characteristics. This technology could be very useful to airport security. To some extent the traditional security procedures such as hand luggage, x-ray and body scans start to look insufficient. Thus, biometrics is considered as a very promising and acceptable technology for airport security to restrict access to secure areas. It is also used in the security screening of passengers during check-in, visitors, and airport personnel.

In Table 3: Acceptance of Biometrics section: Questionnaire) illustrates the various questions asked of passengers to identify their perceptions regarding the acceptance of biometrics devices at the airport and in general context as well.

Acceptance of Biometrics		
Measures	Source	Questionnaire Item
Passenger attitude	Babu, Batta and Lin (2006)	I would allow retinal or facial scans or fingerprints to be taken if it makes the airports safer.
Higher security	Liu and Silverman (2001)	A retinal or facial scan or fingerprints would also ensure a higher security level than using PIN numbers when making a secure transaction on a computer.
Authentication technique	Lui and Silverman (2001)	I would use retinal or facial scans or fingerprints rather than passwords when working on a computer or ATM.
Acceptance	Connolly (2006)	I generally accept the use of devices and systems that do retinal or facial scans or take fingerprints.
Confidence	Gilbert and Wong (2003)	I would have confidence in devices and systems that do retinal or facial scans or take fingerprints.
Passenger security	Tzannatos (2003); Heracleous and Wirtz (2006)	I would approve the use of retinal or facial scan or fingerprints if they increase my own security, for example, assist in the prevention of terrorist attacks.
Confidence	Gilbert and Wong (2003)	I would approve the use of retinal or facial scan or fingerprints if they increase the security of other passengers.
Authentication	Liu and Silverman (2001)	A flight in which the identity of the passengers is confirmed with retinal or facial scan or fingerprints is likely to be safer than one secured using a traditional passport photograph.
Acceptance in check-in	Heracleous and Wirtz (2006)	I would accept using retinal or facial scan or fingerprints if they accelerate the check-in procedure.

Table 3: Acceptance of Biometrics section: Questionnaire

5.13.3. Privacy

Privacy continues to be a very challenging issue and is on top of every individual's agenda. Civil liberties and privacy proponents believe that there are significant issues that need to be solved before biometrics gets the praise it deserves. Factors such as

identity theft and sharing of personal information raise concern among individuals. Moreover, the collection of massive amount of biometric data in databases and their link to government agencies has raised privacy concerns and erosion of civil liberties.

The following questions, listed in Table 4: Privacy section: Questionnaire), which became the privacy dimension of the questionnaire, examined travellers' perceptions regarding sacrificing their privacy right for higher security.

Privacy		
Variables	Source	Questionnaire
Give up privacy to stop terrorisms	Tzannatos (2003); Heracleous and Wirtz, (2006)	I am prepared to give up some rights to privacy if it will prevent terrorist attacks
Give up privacy to prevent theft and defraud	Friedewald, Vildjiounaite, Punie and Wright, (2006)	I am prepared to give up some rights to privacy if it will prevent theft & fraud
Misuse of personal security information	Adey (2004)	There is a possibility that my stored personal security data could be misused for unscrupulous use
Theft of personal data	Connie, Tech, Goh and Ngo (2004)	I am confident that my stored personal security data (for example, retinal or facial scan or fingerprint) can not be stolen
Surveillance	Thomas (2005)	The registration of my personal security data (for example, retinal or facial scan or fingerprint) is generally likely to lead to a high level of surveillance and loss of privacy
Function Creep	Juels, Molnar and Wagner (2005)	I am concerned that facial recognition could be used to track every move I make.

Table 4: Privacy section: Questionnaire

Furthermore, questions like: where the personal data will be stored, who have access to that sensitive biometric data and also, who will share that information; are some of the questions that have been raised in the past. Since a biometrics authentication system uses private details of users, the misuse of biometric data as well as identity

fraud can have far-reaching consequences for the use of biometric technology. Certain biometrics trigger greater perception of privacy invasion among the public than others.

5.13.4. Protecting biometric information

As indicated in chapter 4, biometric technologies can raise privacy concerns as well as enhance privacy. Biometrics is considered by privacy opponents to be the most secure form of authentication technology. Literature reviews have shown that adequate measures of privacy protection of personal data are a basic requirement for the successful deployment of biometric systems. In addition, there are many techniques that can be used to protect biometrics data. For example, encrypting sensitive biometric data can protect privacy of that data.

The questions below (see Table 5: Protecting biometric Information section: Questionnaire.) are asked in order to find out what travellers' opinions are regarding the extent to which they agree or disagree regarding the different measures that are used to protect biometric data.

Protecting Biometrics Information		
Measure	Source	Questionnaire item
Data protection	Loring (2002)	The airline industry should not use passengers' data obtained from retinal or facial scan or fingerprints for any other purposes than originally described.
Enforcement/Redress	Langenderfer and Linhoff (2005)	Passengers must have an avenue of redress if their personal security data is violated.
Unauthorised access	Udo (2001)	Airline industry collecting passengers' data will keep the data secure from unauthorised access.
Confidentiality	Dumortier and Kindt (2005)	Airline industry will inform passengers before putting their personal security data to other use.
Accuracy of data collection	Donos (2005)	Airline industry collecting passengers' data will do so accurately.

Table 5: Protecting biometric Information section: Questionnaire.

5.13.5. Balancing security and privacy

The evolution of technology and its capabilities is continuous and rapid, thus achieving a suitable balance between security and privacy is inevitably a moving target (Casal, 2004). Security and privacy should not be regarded as two extremes as strong security is needed to protect sensitive biometric data. A balance needs to be struck between the two. As mentioned in the previous chapter, security and privacy can co-exist as long as proper guidelines are put in place. Experts are currently working on the issue of finding a balance between security and privacy. One example where a group of professionals met, in order to discuss how a balance can be struck between security and privacy, is at the University of Toronto during the conference entitled "Seeking the middle path" (Randall, 2005).

The items listed in Table 6: Balancing security and privacy) became the item pool of the questionnaire and this section brings a conclusion to the development of the questionnaire.

Balancing security and privacy		
Measure	Source	Questionnaire Item
Delaying check-in procedure	Stibbe (2005)	Devices and systems that do retinal or facial scans or take fingerprints take time. I would accept the application of such systems at check-in time for the benefits of better security.
Speeding check-in procedure	Heracleous and Wirtz (2006)	It takes longer to do retinal or facial scans or take a fingerprint. In the interest of better security at the airport check-in procedure, I would accept: • Less than 15 minutes more • 15 minutes – 30 minutes more • More than 30 minutes more • No preference.
Personal data storage	Bennett (2005)	Personal data from retinal or facial scans or fingerprints needs to be stored somewhere. I would prefer to: ▪ Hold my data personally ▪ Have my data held in a central repository managed by the Airport Company ▪ I have no opinion.
Personal data collection	Zorkadis and Donos, (2004); Bennett (2005)	Personal data needs to be collected. To whom would I be happy to give permission to collect and hold data on my retinal or facial scans or fingerprint: • The government and official institution • Employers • Hospitals & health centres • Data security firms • Commercial organisations • Others.

Table 6: Balancing security and privacy

5.14. Conclusion

In this chapter, the construction of the questionnaire that was used to measure the respondents' attitude towards biometrics, was discussed. Based on the previous chapters and literature reviews, six dimensions were identified, namely Security, Biometrics, Privacy, Protecting biometrics data, and Balancing security and privacy. Many factors, such as a validity and reliability check and avoiding biases so that the

questions in the questionnaire focus directly on the specific issue and provide brevity and clarity, were taken into consideration in order to construct the appropriate questionnaire. The chapter that follows will discuss the statistical analysis of the gathered data.

CHAPTER 6: DATA ANALYSIS

6. Introduction

This chapter presents the analysis of data collected from the survey questionnaire. This chapter presents the results of the empirical study. Data analysis was carried out in two stages: in the first stage, the demographic factors were analysed; in the second stage, reliability and construct validity of independent and dependent constructs were evaluated using Cronbach's alpha coefficient to measure the internal consistency. The last section consists of the statistical analysis that includes the basic statistics, measures of central tendency and reliability of the data.

6.1. Actual Sample (Response rate)

As discussed in chapter 5, in order to evaluate the privacy concerns related to biometrics, the survey instrument was administered to passengers who have travelled internationally by air.

To avoid bias in data collection the same information about the purpose of the survey was provided to each respondent along with a statement about the confidentiality of their responses. After the interview session that took place over couple of days, 137 questionnaires were collected, representing a 91.3% response rate, while 13 questionnaires were left uncompleted.

The high response rate was attributed to the use of simple English questions. Forza (2002) states that the researcher should ensure that in formulating the questions the language of the questionnaire should be consistent with the respondent's level of

understanding. Besides, assurance was given to the passengers that the survey was for their own benefit and that their information will remain anonymous. As for the respondents, they might have appreciated that their welfare and opinions were investigated for their personal safety and security. Also, passengers were allowed to complete the questionnaire on their own, but help was occasionally given to those who experienced difficulty.

Personal reasons were identified as the main factor for those who did not complete the questionnaire. In addition, some of respondents declined to participate because of language barriers.

Once the data collection was completed, it was coded for analysis. One questionnaire was removed from data pool as it did not have any data on one page of the questionnaire. The reason for the missing data could have been that the respondent was tired and missed turning that page.

6.2. Data Coding

The first step in processing data usually entails transcribing the data from the original documents to a computer database (Forza, 2002). However, each questionnaire was given a unique identification number, firstly to avoid duplication of data. In addition, codes were assigned to the demographic information before data were entered into the spreadsheet for analysis. As stated by Kitchenham and Pfleeger (2003), it is sometimes necessary to convert nominal (multiple choice items, checklist), ordinal (forced ranking scale, paired comparison scale) and interval (Likert scale) scale data from category names to numerical scores prior to the data being input into electronic

data files. This was done because SPSS statistical package could not handle categories represented by character strings. As for the Likert scale, coding was rather done during questionnaire design. The coded data were then entered into the spreadsheet. However, a key concern during the survey and the process of data input is handling missing data.

6.3. Missing Data

Before the questionnaires were collected from the respondents it was ensured that all the check boxes were ticked off properly. However, some of the "completed" survey instruments showed some missing values. This could have happened due to respondent fatigue. Thus, in order not to reduce the precision of the calculated statistic due to the missing data, the mean was used to rectify and replace the omitted values. As indicated by Brown and Kros (2003) missing values can be replaced by using the mean of the recorded or available values. In addition, one survey questionnaire was rejected as it indicated more than ten missing values. The reason could have been that the respondent might have mistakenly missed or not turned that page of the questionnaire.

6.4. Demographic Information

Previous research has shown that consumer demographic, economic, and geographic factors played significant roles in determining consumer behaviour (Black, 2005). However, according to Graeff and Homes (2002) very few academic studies have examined the relationship between demographics and consumer privacy concerns, but privacy concerns vary with consumers' age, and gender. Table 8 below provides the

descriptive statistics for the sample. It shows the respondents' demographic information such as gender, age groups, travel frequency, and occupation.

Demographic Profile of Respondents

		Count	Table %
Age	18 - 25 years	N=30	22.1%
	26 - 35 years	N=66	48.5%
	36 - 45 years	N=25	18.4%
	46 - 55 years	N=12	8.8%
	56 years and above	N=3	2.2%
	Total	**N=136**	**100.0%**
Gender	Male	N=93	68.4%
	Female	N=43	31.6%
	Total	**N=136**	**100.0%**
Air travel frequency	Once a month	N=21	15.4%
	Several times a year	N=73	53.7%
	Once a year	N=20	14.7%
	Once in several years	N=22	16.2%
	Total	**N=136**	**100.0%**
Occupation	Working professional	N=94	69.1%
	Student	N=40	29.4%
	Retired	N=2	1.5%
	Total	**N=136**	**100.0%**

Table 7: Demographic Profile

The following section describes in more detail the demographic characteristics of the respondents for this survey:

6.4.1. Age of respondents

There is a likelihood that attitudes to security and privacy will vary with age. As stated by Lu *et al.* (2003), it is important to gain a better understanding of age differences, particularly as it relates to user acceptance and usage of new information technologies. Early adopters of new products are commonly thought to be young and

male in the most technology-led markets (Lu *et al.*, 2003). According to Kolodinsky *et al.* (2004), research has also linked age and adoption of technologies, with younger persons being more likely to adopt. As indicated by Kress, Nancy and Schmid (2000), the real gap in consumer attitudes in the information age is between those who are over 55 years of age and those who are younger. Thus it is important to examine how the different age groups engage in the acceptance of biometrics and deal with the issues surrounding the biometrics application in the airport.

As seen in Table 7 (above), the ages of the passengers ranged from 18 years old to above 56 years old, with the majority, that is, 48.5% aged between 26 to 35 years old.

The second factor, gender, also plays an important role in the acceptance of technologies and the issues, such as privacy and convenience, surrounding emerging technologies.

6.4.2. Gender

Gender is a neglected but important individual variable (Lu, Yu, Liu and Yao, 2003). According to Wahler and Tully (1991), with boys, there is a clear correlation between an interest in technology and attitude towards technology compared to girls. In addition Brosnan, (cited in Gilbert, Lee-Kelley and Barton, 2003), makes the proposition that apparent sex differences are due to the "masculinising" of technology. Thus gender should be taken into considering regarding the concerns and application of biometrics in airport. The former can be used to predict sustained usage behaviour in individual adoption and sustained usage of technology in work places (Lu *et al.*, 2003). Nonetheless, gender has not been found to have a direct effect on

adoption of technology in general, but men and women appear to have different acceptance rates of specific computer technologies, with men more likely to adopt (Kolodinsky, Hogarth, & Hilgert, 2004).

As shown in Table 7: Demographic Profile), the majority of the respondents were males (68.4%) whereas the remaining, that is, 31.4% were females. The T-test was used to test if any significant differences exist between gender and the hypotheses. The next subsection introduces another important measure, that is, travel frequency, to better understand travellers behaviour with respect to privacy, convenience, and acceptance of biometrics.

6.4.3. Travel frequency

With regard to convenience, the use of biometrics for identification of passengers at airports benefits frequent travellers by enabling them to get through security checkpoints by accelerating the security process (Woodcock, 2005). According to Bailey, (cited in Woodcock, 2005), in America those travellers willing to hand over biographical and biometric information to the Transportation Security Administration, have an expedited trip through security. It is important to determine if there exist any differences in the acceptance of biometrics, sacrificing of privacy, and convenience among the different air travel frequency groups. Hence, air travel frequency is used to test the three hypotheses.

From the observations in Table 7: Demographic Profile), the bulk of the travellers, that is, 53.7% travel several times a year followed by 14.7%, 15.4%, and 16.2% who

travel "Once a year", "Once a month", and "Once in several years" respectively. The final section describes the occupation of the respondents.

6.4.4. Occupation

Occupation can be used to get an insight into who is more likely to be concerned about informational privacy and acceptance of biometrics. As stated by Joinson and Paine (2006), the level of privacy concern might differ between people as different people have different levels of concerns about their privacy. Data collected from four different groups are described below.

The majority of respondents were from the working environment (69.1%), followed by students (29.41%). The number of retired was just 1.47% whereas there were no respondents that were unemployed.

The next section describes the public knowledge regarding fingerprints and the various biometrics currently present on the market.

6.5. Biometrics' knowledge

It is important to establish the previous exposure that a respondent has had to biometric applications. The figure below summarises the respondent's previous related knowledge of biometrics.

"Frequency" is the number of respondents, "percent" is the percentage of respondents. The x-axis indicates the technology concerned, and the y-axis shows the frequency of respondents exposed to that technology.

	Frequency	Percent	Cumulative Percent
Fingerprint	80	58.8	58.8
Retinal Scan	1	.7	59.6
Hand Geometry Scan	1	.7	60.3
Facial Recognition	4	2.9	63.2
None	11	8.1	71.3
Fingerprint & Retinal	1	.7	72.1
Fingerprint & Iris	3	2.2	74.3
Fingerprint & Hand Geometry	10	7.4	81.6
Fingerprint & Facial	17	12.5	94.1
Fingerprint & Retinal & Iris	1	.7	94.9
Fingerprint & Retinal & Hand Geometry	2	1.5	96.3
Fingerprint & Retinal & Facial	1	.7	97.1
Fingerprint & Iris & Facial	1	.7	97.8
Fingerprint &Retinal & Iris & Hand Geometry	3	2.2	100.0
Total	136	100.0	

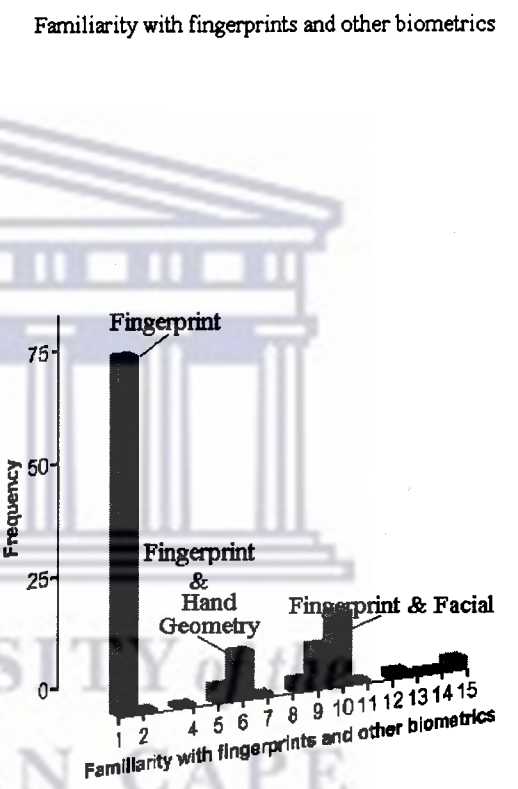


Figure 8: Knowledge about fingerprints & other biometrics

Figure 8 shows previous knowledge of travellers about biometrics and something they have given out, for example, having their fingerprints taken to obtain a passport. By far, the majority of the respondents, more than 58%, had had a fingerprint taken before. Of these, many have also had exposure to facial and hand biometrics.

It is also clear from Figure 8: Knowledge about fingerprints & other biometrics), that very few travellers have used other forms of biometrics, thus indicating that the level of knowledge among travellers regarding biometrics is low in South Africa.

Security and privacy are the focal point of this research, hence it is important to identify to what extent passengers rate their experiences and the events that took place in the past and that could happen in future at the airport. Therefore, all the items related to general security are explained first below.

6.6. General security (items 9-14)

These items were generated based on the literature review. Table 8: General security dimension) shows the different items that were used to measure passengers' point of view of airport security. These items were analyzed on a single item basis.

General Security	
Item #	Measurement
9	There is a serious threat that airport terrorist attacks that have occurred in the past, could happen again
10	The airline industry is liable (has a legal responsibility) for protecting passengers from terrorist attacks
11	All airline and airport personnel should be screened to ensure they have no criminal record
12	I have full confidence in the ability of the passenger screeners to keep air travel secure from hostile individuals
13	Security staffs using X-rays screen hand-luggage effectively
14	I am more concerned about safety than my personal rights – for example, I do not object to being searched

Table 8: General security

Next the dimensionality, reliability, and construct validity of the questionnaire are taken into account.

6.7. Construct reliability

The instrument developed for this study is composed of multiple items for each dimension. The items for the acceptance of biometrics and privacy dimension were taken directly from Bente *et al.* (2005) whereas the dimension "protecting biometrics information" has its source in the literature review. The 6-point Likert scale was used to measure travellers' attitude, preferences, and subjective opinions for these dimensions. Once the items were placed in their respective dimensions they were tested for internal consistency to estimate how consistently respondents answer to the items.

Cronbach's α was used to measure the reliability of each dimension. This coefficient ranges from 0 to 1 and a score of 0.7 is considered an acceptable reliability coefficient. According to Liu and Arnett (1999), a low value of Cronbach's alpha (that is, close to 0) implies that the variables are not internally consistent.

6.7.1. Acceptance of biometrics dimension (15-23)

The attitude towards the acceptance was evaluated as biometrics plays a significant role in the authentication of passengers in developed countries. As stated by Bente *et al.* (2005), acceptance of biometrics characterizes a user's attitude, perceived enhancement of general security.

The 9 items, shown in Table 9: Acceptance of Biometrics dimension) consist of different statements regarding the acceptance of biometrics in a broader sense.

Acceptance of biometrics
I would allow retinal or facial scans or fingerprints to be taken if it makes the airports safer
A retinal or facial scan or fingerprints would also ensure a higher security level than using PIN numbers when making a secure transaction on a computer
I would use retinal or facial scans or fingerprints rather than passwords when working on a computer or ATM
I generally accept the use of devices and systems that do retinal or facial scans or take fingerprints
I would have confidence in devices and systems that do retinal or facial scans or take fingerprints
I would approve the use of retinal or facial scan or fingerprints if they increase my own security, for example, assist in the prevention of terrorist attacks
I would approve the use of retinal or facial scan or fingerprints if they increase the security of other passengers
A flight in which the identity of the passengers is confirmed with retinal or facial scan or fingerprints is likely to be safer than one secured using a traditional passport photograph
I am concerned that facial recognition could be used to track every move I make

Table 9: Acceptance of Biometrics

According to Bente *et al.*. (2005), biometrics is used in private and public environments. The latter can thus have an impact on the acceptance of biometrics. Items 15, 20, 21, 22, and 29 describe the use of biometrics for improving airport security. Item 16 and 17 describe the use of biometrics in different applications. Item 18 explains the general acceptance of biometric for enhanced security. Finally, item 19 was used to measure respondents' confidence regarding biometrics.

Reliability analysis was then carried out once all items were identified for "Acceptance of Biometrics" dimension.

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
Item 15	38.11	58.277	.603	.829
Item 16	38.48	55.348	.682	.819
Item 17	38.55	54.486	.644	.825
Item 18	38.31	62.111	.462	.843
Item 19	38.43	60.454	.570	.832
Item 20	37.96	58.021	.772	.815
Item 21	37.93	58.839	.743	.818
Item 22	38.13	61.242	.545	.835
Item 29	39.04	66.665	.195	.872

Reliability Statistics

Cronbach's Alpha	N of Items
.849	9

Table 10: Cronbach's Alpha of Acceptance of Biometrics Dimension

As indicated in Table 10: Cronbach's Alpha of Acceptance of Biometrics Dimension) no item was deleted from this dimension. A high α, as indicated in Table 10: Cronbach's Alpha of Acceptance of Biometrics Dimension), of greater than 0.8 in this dimension indicates high internal consistency. As mentioned by Bente *et al.* (2005) an alpha exceeding 0.8 is in general sufficient for a scale that is measuring one single concept, indicating that all items were answered in the same way and are therefore measuring the same concept.

6.7.2. The privacy dimension (items 24-29)

The second dimension which consisted of privacy concerns was analyzed next. The items used here are those items that were found to explain privacy concern using biometrics.

Individuals have the right to control what information about them should or should not be communicated to others and under what circumstances. Misuse of biometric data can lead to invasion of informational privacy through secondary uses. Table 11 illustrates the privacy dimension.

Privacy Concerns	
Item #	
24	I am prepared to give up some rights to privacy if it will prevent terrorist attack
25	I am prepared to give up some rights to privacy if it will prevent theft & fraud
26	There is a possibility that my stored personal security data could be misused for unscrupulous use
27	I am confident that my stored personal security data (for example, retinal or facial scan or fingerprint) cannot be stolen
28	The registration of my personal security data (for example, retinal or facial scan or fingerprint) is generally likely to lead to high levels of surveillance and loss of personal privacy
35	Devices and systems that do retinal or facial scans or take fingerprints take time. I would accept the application of such systems at check-in time for the benefits of better security

Table 11: Privacy concerns dimension

The privacy dimension consists of different items measuring the same concept. Items 24 and 25 are related to the rights to privacy as described in chapter 1. Items 26, 27, 28, and 35 are related to biometrics and explain the unauthorised data collection, storage and use which give could give rise to informational privacy if accessed by unauthorised individuals.

This module initially consisted of 6 items, as shown below (Table 12: First reliability analysis of privacy dimension), having an α of 0.594. The first analysis indicated that by deleting item number 26, "*There is a possibility that my stored personal security data could be misused for unscrupulous use*", from the dimension the internal consistency could be increased.

The reason for the low Cronbach's alpha may be due to the confusing question. It could be more useful to rephrase the question (item 26) in a simpler form. The word "dishonest" could have been used instead of "unscrupulous".

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
Item 24	21.88	15.127	.656	.380
Item 25	21.85	16.532	.591	.426
Item 26	21.38	24.475	.006	.658
Item 27	22.78	20.514	.203	.607
Item 28	22.00	20.800	.244	.584
Item 35	21.54	20.472	.325	.552

Reliability Statistics

Cronbach's Alpha	N of Items
.594	6

Table 12: First reliability analysis of privacy dimension

In Table 13, after item 26 was deleted, the Cronbach's Alpha increased to 0.658. As suggested by Mansfield (2005) in order to not sterilise the instrument or discard what might prove to be valuable concepts, a cut-off can be made at 0.6.

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
Item 24	16.98	13.888	.647	.479
Item 25	16.94	15.359	.569	.529
Item 27	17.88	17.340	.329	.647
Item 28	17.10	19.939	.184	.701
Item 35	16.64	18.484	.367	.626

Reliability Statistics

Cronbach's Alpha	N of Items
.658	5

Table 13: Final Analysis of Privacy Dimension

6.7.3. Protecting Biometrics Information Dimension (Items 30-31)

The third dimension consists of "Protecting biometrics information". As described in chapter 4, adequate measures of privacy protection of personal data are a basic requirement for the successful deployment of biometric system.

The literature has shown that biometrics offer enhanced security. However, these technologies also raise privacy concerns. Security and privacy associated with biometrics have become important issues in today's society. Two extremes exist regarding security and privacy. At one extreme there is less of security and more of privacy, and at the other end it is the inverse.

The literature review has shown that in some countries travellers want more security but not at the expense of privacy. Therefore, it is essential to find out how security can be balanced with privacy in order to get a larger group of people to accept the use of biometrics in airports. As Casal (2004) suggests, maintenance of the database, and its integrity, security and protection are sensitive issues and therefore achieving a suitable balance between security and privacy is possibly a moving target.

Table 14 shows the set of items related to the collection, use, and sharing of biometrics data and that are associated with the fair information practices principles.

Protecting biometrics information	
Item #	
30	The airline industry should not use passengers' data obtained from retinal or facial scan or fingerprints for any other purposes than originally described
31	Passengers must have an avenue of redress if their personal security data is violated
32	Airline industry collecting passengers' data will keep the data secure from unauthorised access
33	Airline industry will inform passengers before putting their personal security data to other use
34	Airline industry collecting passengers' data will do so accurately

Table 14: "Protecting biometrics information" dimension

Fair information practices principles can help strike an appropriate balance between security and protecting the privacy of individuals. These principles include:

- Awareness - An awareness that personal biometrics data are being collected;
- Choice - How the collected personal data is used;
- Access - Individual's ability to access his or her personal data;
- Integrity – Organisation should ensure that data collected are accurate and secure from unauthorised access; and
- Redress – Have an avenue of redress for violation.

The reliability coefficient was then computed once all the items have been identified for this dimension.

Table 15 (below) presents the first reliability analysis of the "Protecting biometrics information" dimension with a Cronbach's α of 0.676.

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
Item 30	19.63	16.666	.125	.734
Item 31	19.38	17.290	.209	.698
Item 32	20.33	11.008	.635	.520
Item 33	20.39	10.121	.588	.542
Item 34	20.54	10.932	.616	.528

Reliability Statistics

Cronbach's Alpha	N of Items
.676	5

Table 15: First reliability analysis of "Protecting biometrics information"

As indicated below in table 16, two items (item 30 = *The airline industry should not use passengers' data obtained from retinal or facial scan or fingerprints for any other*

purposes than originally described, and item 31 = *Passengers must have an avenue of redress if their personal security data is violated*), were removed from this dimension due to low internal consistency.

The inconsistent answers may have been due to the fact that the respondents might have misunderstood or misinterpreted the questions. Concerning item 30, instead of using "retinal or facial scan or fingerprints" simply using "personal security data" could have influence the respondents' answer. With regard to item 31, travellers might have misunderstood the meaning of "avenue of redress". Thus, by rephrasing or reformulating the questions a better response may have been obtained.

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
Item 32	9.21	7.676	.726	.719
Item 33	9.26	6.996	.653	.796
Item 34	9.41	7.770	.677	.764

Reliability Statistics

Cronbach's Alpha	N of Items
.825	3

Table 16: Final reliability analysis of "Protecting biometrics information"

As a result, the internal consistency, as measured by Cronbach's α, of the 3 items was 0.825 after the 2 items were deleted from the dimension (as seen in table 17 above).

6.7.4. Convenience (item 23)

As shown in Table 17, this single item was used to measure if passengers were willing to sacrifice privacy for convenience.

Convenience	
Item #	
25	I would accept using retinal or facial scan or fingerprints if they accelerated the check-in procedure

Table 17: Convenience Dimension

Biometric, which contains sensitive information about people, carry with it informational privacy concerns due to an individual's inability to control his/her personal information from misuse. This item is used to measure if travellers are voluntarily willing to sacrifice some of their personal information for convenience, such as getting through security checkpoint faster at the airport.

6.8. Hypothesis Testing

After the data were analyzed using Cronbach's α, it was presented, using Microsoft Excel, in the form of figures and tables for each hypothesis to facilitate the evaluation of respondents' attitude towards the three dimensions.

1. The figures consist of a histogram and a pie-chart.
    1.1. Firstly, the histograms show the percentage of respondents expressing their opinion, that is, their degree of agreement and disagreement, on a six-point Likert scale for items that form the three dimensions, namely: acceptance of biometrics, sacrificing privacy for higher security, and sacrificing privacy for convenience, and
    1.2. Secondly, a pie-chart resulted from collapsing the six-point Likert scale into two groups, "Agree" and "Disagree" as shown in the figures below, in order to further analyze the results.

2. The tables show the means and standard deviations of demographic characteristic of respondents, and their significant difference with regards to the hypotheses.

For hypothesis testing, ages were adjusted into 3 groups using a SPSS tool:

- Group 1 (n=96) were between 18 and 35 years of age
- Group 2 (n=37) were between 36 and 55 years of age
- Group 3 (n=3) were 56 years or older.

The following section presents the data graphically as generated in Microsoft Excel. The three hypotheses were described by means of graphs and indicate whether they support the specific aims of this research and answer the questions raised in chapter one.

6.8.1. Hypothesis 1:

Biometric Security Measures at Airports are positively accepted by Travellers

Security at the airport is regarded as a very essential topic among travellers. Biometrics has been identified as a solution to this problem. According to Heracleous and Wirtz (2006) biometrics can offer significant security enhancements as well as other value-added applications.

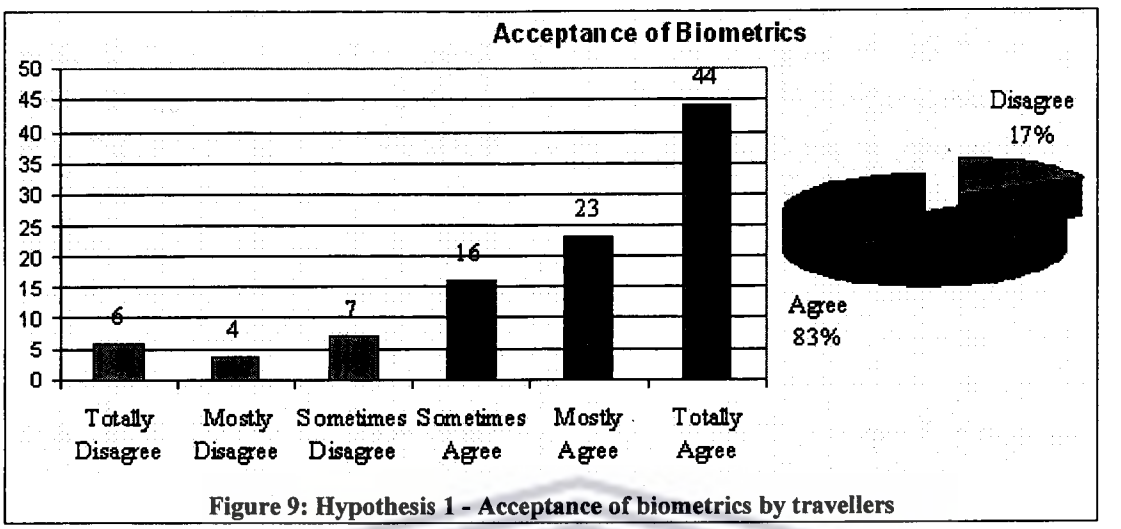


Figure 9: Hypothesis 1 - Acceptance of biometrics by travellers

In this research, the survey showed that 83 % of respondents have a positive attitude towards the acceptance of biometrics (see figure 9 above), whereas 17 % are against the application of biometrics at the airport. Thus we accept hypothesis 1.

Finding: These results demonstrate strong support in favour of Hypothesis 1.

6.8.1.1. Age

The "F" test was used to analyse the significant difference between age and the 1st hypothesis.

Table 18 shows the age of the respondents.

Age	Mean 1	Standard Deviation	Number of Respondents	F (ANOVA test)	P value
Group 1	4.7477	0.86930	96	0.391	P > 0.05
Group 2	4.8468	1.17073	37		
Group 3	5.4815	0.39021	3		

Table 18: Age (Acceptance of Biometrics)

In group 1, consisting of 96 travellers, with a mean of 4.7 and a standard deviation (S.D) of 0.8. In group 2, there was 37 travellers (mean=4.8, S.D=1.0). And in the last group, which has only 3 travellers, the mean was 5.4 with S.D 0.3.

Finding: After the adjustment, there was no statistical significant difference (P>0.05) between the age groups regarding the acceptance of biometrics for security measures at the airport.

6.8.1.2. Gender

As indicated by Knupfer and Rust, (cited in Schimmel & Nicholls, 2003), gender differences exist in both technology acceptance and usage behaviour.

Gender	Mean	Standard Deviation	Number of Respondents	T-value	P-value
Male	4.7145	0.99494	93	0.171	P > 0.05
Female	4.9561	0.85040	43		

Table 19: Gender (Acceptance of Biometrics)

Therefore, as shown in the table above, the mean value for males and females were 4.7 and 4.9 respectively. Also there was not much difference in the standard deviation as for males it was 0.9 and for females it was 0.8. The "t" value is 0.171 (P>0.05)

Finding: There is no significant difference in the attitude between genders regarding the acceptance of biometrics for security measures at the airport.

6.8.1.3. Air Travel Frequency

Table 20 shows, in the "Once a month" group there were 21 respondents with mean 4.3 and S.D 1.3. In the "Several times a year" category, there were 73 travellers with mean 4.9 and S.D 0.8. Twenty passengers with mean 4.6 and S.D 0.9 have travelled once a year. And in the last group there were 22 people with mean 4.8 and S.D 0.8, and who have travelled once in several years.

Air Travel Frequency	Mean 1	Standard Deviation	Number of Respondents	ANOVA	P value
Once a month	4.3810	1.30742	21	0.103	P > 0.05
Several times a year	4.9239	0.85704	73		
Once a year	4.6222	0.91724	20		
Once in several years	4.8939	0.83040	22		

Table 20: Air travel frequency (Acceptance of biometrics)

Finding: There is no significant difference between the number of times people travel and acceptance of biometrics.

6.8.1.4. Occupation

Occupation	Mean 1	Standard Deviation	Number of respondents	ANOVA	P value
Working Professional	4.7742	0.98204	94	0.759	P > 0.05
Student	4.8056	0.91867	40		
Retired	5.2778	0.23570	2		

Table 21: Occupation (Acceptance of biometrics)

Table 21 shows that out of the 136 respondents, 94 were working professionals, 40 were students, and only 2 retired. In this table the mean and standard deviation of the

different groups are indicated. Results from the one-way ANOVA revealed no significant differences between the groups and the acceptance of biometrics at the airport.

Finding: There is no significant difference between professional groups regarding the acceptance of biometrics at the airport.

6.8.2. Hypothesis 2

Passengers will sacrifice privacy for higher security

Berscheid argues, (cited in Metzger, 2004), that individuals differ in the degree to which they desire and value personal control over information about themselves. With regard to information privacy values, studies have found a negative relationship between the value people place on and perceptions of control over personal information (Metzger, 2004).

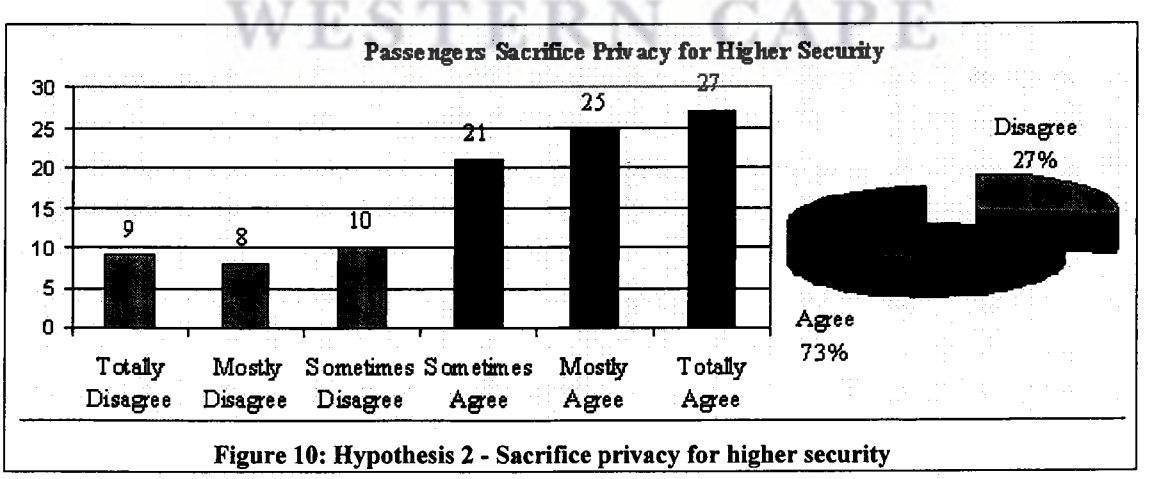


Figure 10: Hypothesis 2 - Sacrifice privacy for higher security

Figure 10: Hypothesis 2 - Sacrifice privacy for higher security) indicates that the data support the hypothesis as most of the travellers are willing to sacrifice privacy for

higher security through the use of biometrics. 73% agreed to use biometrics at the airport compared to 27% who disagreed. Hypothesis 2 is therefore accepted.

6.8.2.1. Age

Various studies carried out by Campbell, Milner *et al.*, (cited in Brown & Muchira, 2004), have found that age is an important factor in analyzing privacy concerns since younger age groups tend to have lower privacy concerns than old age groups.

Age	Mean 2	Standard Deviation	Number of Respondents	(ANOVA test)	P value
Group 1	4.2250	1.00116	96	0.186	P > 0.05
Group 2	4.3297	0.96404	37		
Group 3	5.2667	0.30551	3		

Table 22: Age (Sacrifice privacy for higher security)

Finding: In this research, there appears to be no significant difference between the three groups in connection with sacrificing privacy for higher security (see Table 22). The 3 groups of individuals are prepared to sacrifice their individual's rights to privacy for higher security to strengthen airport safety measures as the statistic shows that "F" = 0.186 (P>0.05).

6.8.2.2. Gender

According to Cozby, Derlega, Metts, Petronio, and Margulis, cited in (Metzger, 2004), differences in both the amount and topics of self-disclosure between males and females have been observed in the literature on interpersonal communication. According to Derlega *et al.*, (cited in Metzger, 2004), women have been found to disclose both more and more intimate information than men, although this finding depends on the specific social context of the disclosure.

Gender	Mean 2	Standard Deviation	Number of Respondents	T value	P value
Male	4.1763	0.99601	93	0.083	P > 0.05
Female	4.4930	.95054	43		

Table 23: Gender (Sacrifice Privacy for Higher Security)

Finding: With regards to sacrificing privacy for higher security, for this research, there exists no significant difference in gender as Table 23 shows. The data analysis shows that males and females with mean 4.1 and 4.4, and S.D 0.9 respectively resulted in no significant difference as "t" value is 0.083 (P>0.05).

6.8.2.3. Air travel frequency

With respect to their travel frequencies, the respondents were asked if they will sacrifice privacy for higher security.

Air Travel Frequency	Mean 2	Standard Deviation	Number of Respondents	ANOVA	P value
Once a month	4.0952	1.23874	21	0.367	P > 0.05
Several times a year	4.4000	0.91287	73		
Once a year	4.0200	1.06207	20		
Once in several years	4.2727	0.89771	22		

Table 24: Air Travel Frequency (Sacrifice Privacy for Higher Security)

Finding: According to Table 24, there was no significant difference (F=0.3, that is, P>0.05) between respondents who travel once a month (mean=4.0, S.D=1.2), several times a year (mean=4.4, S.D=0.9), once a year (mean=4.0, S.D=1.0), and once in several years (mean=4.2, S.D=0.8) with regard to giving up privacy for advanced security.

6.8.2.4. Occupation

As stated by Sheehan (2002), the individual's orientation to privacy concern may be influenced by their age and their level of education. Persons with higher levels of education are more concerned about their privacy online than persons with less education (Sheehan, 2002).

Occupation	Mean 2	Standard Deviation	Number of respondents	ANOVA	P value
Working Professional	4.3191	0.98169	94	0.198	P > 0.05
Student	4.1250	1.00224	40		
Retired	5.3000	0.42426	2		

Table 25: Occupation (Sacrifice privacy for higher security)

Finding: Table 25 shows that there were no significant difference (F=0.198, that is, P>0.05) between working professional, student, and retired.

6.8.3. Hypothesis 3:

Passengers will sacrifice privacy for convenience

Convenience may allow travellers to avoid long security lines and accelerate check-in procedures. As stated by Kroeker (2002), biometrics effectively trades some amount of privacy and cost effectiveness for ultimate convenience. Biometric systems, which will start impacting people's lives over the next 2 to 5 years, will manifest themselves in government projects, aviation security, and fraud-reduction programs, and offer an enormous amount of convenience to users (Kroeker, 2002).

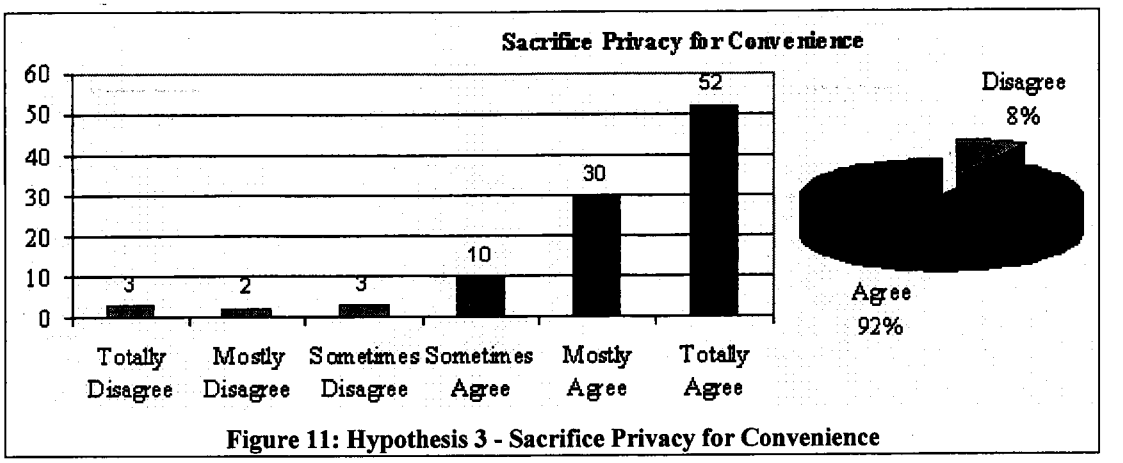


Figure 11: Hypothesis 3 - Sacrifice Privacy for Convenience

An individual's rights to privacy are an important concern to travellers. Despite this fact, the majority of the respondents (92%) agree compared to 8% who disagree, as being prepared to reveal their personal information in exchange for convenience (see Figure 11: Hypothesis 3 - Sacrifice Privacy for Convenience).

Thus, the third hypothesis is accepted and concluded that travellers are willing to sacrifice their own privacy in return for increased convenience. Thus, biometrics is seen as a technology that can beef up airport security and also provide convenience by allowing passengers to bypass lengthy and time-consuming security check-points at the airport.

6.8.3.1. Age

One-way ANOVA (analysis of variance) was use to determine whether there were significant difference between the difference age groups. Group 1 with 96 respondents has mean 5.2 and S.D 1.0, group 2 has mean 5.0 and S.D 1.4, and the mean and S.D for group 3 were 6.0 and 0.0 respectively.

Age	Mean 3	Standard Deviation	Number of Respondents	F value (ANOVA test)	P value
Group 1	5.2083	1.04546	96	0.382	P > 0.05
Group 2	5.0541	1.48970	37		
Group 3	6.0000	0.00000	3		

Table 26: Age (Sacrifice Privacy for Convenience)

Finding: According to Table 26, there was no significant difference between the 3 age groups for sacrificing privacy for convenience.

6.8.3.2. Gender

The t-test was used to determine whether there was significant difference between genders.

Gender	Mean 3	Standard Deviation	Number of Respondents	T value	P value
Male	5.1290	1.27028	93	0.426	P > 0.05
Female	5.3023	0.93948	43		

Table 27: Gender (Sacrifice Privacy for Convenience)

Finding: The result shows that there was no significant difference between male (mean=5.1, S.D=1.2) and female (mean=5.3, S.D=0.9) about sacrificing privacy for convenience (see Table 27).

6.8.3.3. Air travel frequency

Air Travel Frequency	Mean3	Standard Deviation	Number of Respondents	ANOVA	P value
Once a month	4.5714	1.80476	21	0.032	P < 0.05
Several times a year	5.3151	0.95564	73		
Once a year	5.0000	1.29777	20		
Once in several years	5.5000	0.74001	22		

Table 28: Air Travel Frequency (Sacrifice Privacy for Convenience)

Finding: Table 28 indicates that there was a significant difference (F=0.032, that is, P<0.05) with regards to air travel frequency and passengers sacrificing privacy for convenience. Respondents travelling "once a month" have a mean of 4.5 and a S.D of 1.8 compare to the other groups with mean 5.0 or above and S.D below 1.3, meaning that they are a bit reluctant to give up privacy for convenience.

The reason could be, as stated by Rhodes (2003), that people might find biometric technologies difficult, if not impossible, to use. Still some might resist biometrics because they believe them to be intrusive, inherently offensive, or just uncomfortable to use. In addition, respondents who travel frequently might assume that with convenience one thing can go wrong, and that is "function creep". With the latter, systems designed for one purpose are extended over time to other purposes not originally intended (Wright, 1994).

6.8.3.4. Occupation

One-way ANOVA was used to make comparisons between working professionals, students, and retired.

Occupation	Mean3	Standard Deviation	Number of respondents	ANOVA	P value
Working Professional	5.1489	1.24397	94	0.581	P > 0.05
Student	5.2250	1.02501	40		
Retired	6.0000	0.0000	2		

Table 29: Occupation (Sacrifice Privacy for Convenience)

Finding: Table 29 indicates that no significant difference (F=0.5) were observed, in table 21, for working professionals (mean=5.1, S.D=1.2), students (mean=5.2, S.D=1.0), and retired (mean=6.0, S.D=0).

The next part describes three additional items that were part of the survey questionnaire. These items were analysed on a single item basis. The first item was used to evaluate respondents' attitude towards any additional time that might be caused by the use of biometrics for checking procedures. And lastly, the two extra items that were analysed were data storage and data collection that give rise to privacy concerns.

It is also important to get an understanding of issues relating to extended time, data storage, and data collection of personal biometrics data.

6.9. Acceptance of additional time

Biometrics reduce the time required for check-in of passengers. For example, at the Schiphol airport biometrics allows enrolled passengers to bypass busy queues and

check-in delays, and simultaneously gives more time for additional security measures to be placed upon those not enrolled in the biometric scheme (Adey, 2004).

However, the assumption was made that it may take longer to do retinal or facial scans or take fingerprints in the interest of better security at the airport check-in procedure. The question, using item 36 (*It takes longer to do retinal or facial scans or take fingerprints. In the interest of better security at the airport check-in procedure, I would accept*), was asked in order to determine respondents' attitude despite the possible inconvenience of extended time.

		Count	Table %
Item 36	Less than 15 minutes more	N=92	67.6%
	15 minutes - 30 minutes more	N=16	11.8%
	More than 30 minutes more	N=3	2.2%
	No Preference	N=25	18.4%
	Total	**N=136**	**100.0%**
Item 37	Hold my data personally (e.g. on a smart card)	N=88	64.7%
	Have my data held in a sentral repository managed by ACSA	N=27	19.9%
	I have no opinion	N=21	15.4%
	Total	**N=136**	**100.0%**
Item 38	Government and Official Institutions	N=53	39.0%
	Employers	N=3	2.2%
	Hospitals and Health Centres	N=13	9.6%
	Data Security Firms	N=31	22.8%
	None	N=36	26.5%
	Total	**N=136**	**100.0%**

Table 30: Data Processing Time, Storage & Collection

The behaviour of passengers regarding the extended waiting time is presented in Table 30, at the airport for better security were as follows:

- 2.2% of passengers indicated that they would not mind 30 minutes more of extra waiting time for better security.
- 18.4% have no preference regarding the wait time for better security.
- 11.8% pointed out that they would spend between 15 minutes to 30 minutes more for check-in procedure.
- Finally, the highest number of respondents, that is, 67.6% showed that they would spend less than 15 minutes more.

One key concern associated with biometrics and that gives rise to privacy concern is who should collect biometrics data.

6.10. Personal Data Collection

As stated by Whisenant (2003), the concern raised by the privacy proponent is the collection of an individual's personal biometric data that can allow monitoring the movement of free citizens.

As shown in Table 30: Data Processing Time, Storage & Collection) the majority of the respondents are 39% suggested that they would be happy to give government the permission to collect and hold their biometric data. The reason that might have encourage respondents for such an action could be, as indicated by Mc Cullagh (2005:9), that government would inform the citizens precisely when information is to be collected and for exactly what purposes. Whereas, the reason the remaining respondents are reluctant to permit government to collect and hold there biometric data could be of the fear that their movement would be constantly monitored.

On the other hand, just above 2% respondents indicated that they would permit employees to collect their personal data. This might perhaps be for the reason that employee mistakes can easily lead to the following (Teng, 2005):

1. Revelation of classified data, that is, leaving data in unprotected areas, such as desktop,
2. Entry of erroneous data,
3. Accidental deletion or modification of data,
4. Storage of data in unprotected areas, and
5. Failure to protect information.

Once the personal data has been collected, it is also important to determine where respondents would prefer to store their sensitive data in order to restrict secondary uses and identity theft.

6.11. Data Storage

As indicated in chapter 3, one of the factors that gave rise to privacy concerns is the storage of personal biometric data. As stated by Bente *et al.* (2005), when it comes to introducing a biometric system the question always arises where the data should be stored. Should it be stored in a central database or on a smartcard.

65% of the respondents would prefer to store their personal security data on a smart card, whereas 19.9% indicated that they would not mind having their data held in a central repository managed by ACSA, while the remaining 15% do not have any opinion about their data storage.

According to Bente *et al.* (2005), reasons for having no opinion about data storage could be:

1. That people generally need more information about data storage and data security in order to estimate risks and chances of different ways of data protection; and/or
2. That they have to pay for a smart card.

It is important that stored biometrics data are accessible by the authorised users only. Concerns have been raised regarding the centralised storage of data. These data are subject to secondary uses and identity theft. Fair information practices may help the protection of personal information.

6.12. Protecting Biometrics Information

Rose (cited in Gopal *et al.*, 2006), defines privacy information as "information that is produced privately and can be hidden". Transacting on private information requires careful consideration of privacy which is the "right of an individual, group, or institution to determine when, how and for what purpose information concerning himself or itself can be collected, stored and released to other people or entities" (Gopal *et al.*, 2006). Threats to data privacy can come from inside (accidental disclosure, insider curiosity and subordination) as well as the outside (uncontrolled secondary usage) each organisation (Karjoth & Schunter, 2002).

The fair information practices are related to elements of the Privacy Act of 1974, and state that individuals have rights pertaining to the collection, access, and use of information about themselves, and that organisations and managers of systems are

responsible for the damage done by systems to individuals' privacy (Gopal *et al.*, 2006).

Respondents were asked to rate their level of agreement related to the collection, use, and sharing of biometric data in the airport context.

Shown in Figure 12: Protecting Biometrics Information) 76% travellers agreed that issue related their personal data will be communicated to them by the airlines. The chapter is concluded by stating that respondents have confidence that their personal data will not be misused or disclosed to third party, and will be kept secure by the airline.

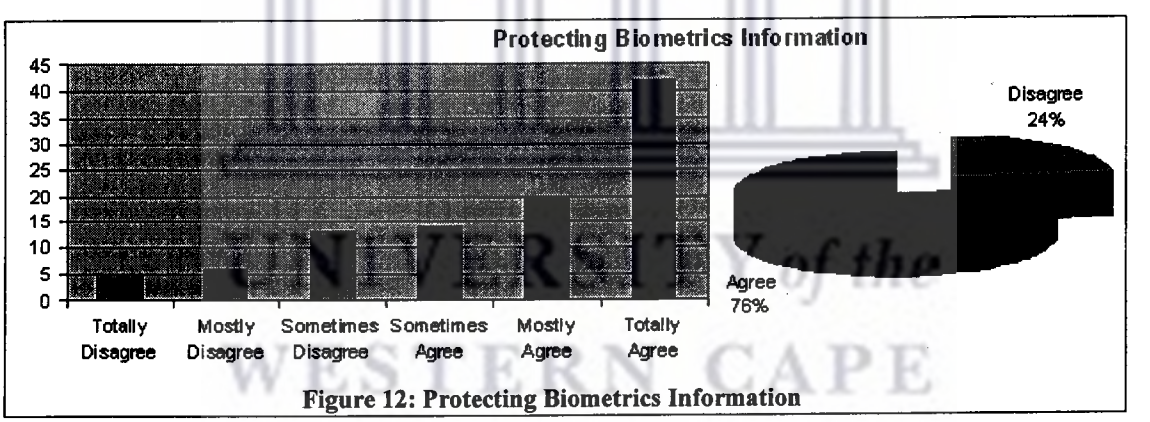


Figure 12: Protecting Biometrics Information

6.13. Conclusion

The results of the data analysis have been presented. First of all the demographic data was analyzed. Then Cronbach's α was estimated for each dimension. Regarding the privacy dimension, one item was deleted to improve the coefficient α.

The aim of this research was to evaluate the privacy concerns regarding biometrics recognition and understand whether the security benefits associated with biometrics

outweigh privacy concerns. The data collected during survey was used to test the hypotheses. The three null hypotheses are accepted and it is postulated that respondents will give up privacy for higher security and convenience. Also, travellers will accept biometrics security measures at the airport despite privacy concerns.

Three additional items were added to the survey questionnaire to evaluate respondents' attitude regarding issues surrounding biometrics, namely; additional time for screening purposes, personal data collection, and data storage.

- Firstly, most passengers would be prepared to spend no more than 15 minutes more at the check-in procedure.
- Secondly, passengers would permit government to collect and hold their biometric data.
- And lastly, respondents would prefer to store their personal security data on a smart card rather than have it held in a central repository.

The next chapter provides a concluding overview and identifies areas for future research.

CHAPTER 7: CONCLUSION

7. Introduction

This chapter brings to an end this research project. It makes a number of concluding comments about the investigation into attitudes of air travellers. The research focused on the security and privacy issue with regard to the use of biometrics technology at airports.

The aim of the research was to evaluate privacy concerns regarding the use of biometrics at the airport and to understand whether the security benefits associated with biometrics outweigh privacy concerns. The aim was to help Information Systems management at ACSA (Airport Company of South Africa) better understand travellers' perceptions of integrating biometrics and measuring their attitude towards the application of biometrics in security.

The survey was carried out by administering questionnaires to people who have travelled internationally, are aware of the security issues and have had personal experience of security at airports.

The generation of a reliable research instrument consisting of dimensions such as privacy concerns, acceptance of biometrics, and convenience were consistent with the literature and very useful to answer each of the research questions mentioned below.

7.1.Research Questions

There are many issues associated with the use of biometrics. For this research the concerns involved security and privacy. The latter is regarded as a basic human right that allows the individual to gain access to his or her personal data, and knowledge about how their data is collected, used, and retained. The focus of the research was on three key questions, specifically:

- Will travellers accept biometric for higher security measures?
- Will passengers be willing to opt for higher security measures by giving up some privacy?
- Will passengers sacrifice privacy for convenience?

7.2.Literature Review

o Airport Security

Terrorist attacks are a serious threat to all individuals. The safety and security of every South African citizen is a major factor to be concerned, especially when taking into consideration that the 2010 Soccer World Cup will be held here. Advanced technologies need to be used to track and stop criminals. Current security checkpoints are imperfect. Many factors have been associated with the problem. One of them is human error, that is, physical and/or mental error. Even in the best of circumstances due to the repetitive nature of security work, loss of concentration, distraction, and fatigue mistake is inevitable. As a consequence, the ineffective passenger and luggage screeners could contribute to a terrorist attack. One technology than offers greater security is biometrics. Biometrics is the automatic authentication of an individual and it provides advanced ways of identifying passengers.

- **Biometrics**

There has been growing interest in the use of biometrics to combat against terrorist attacks, identity theft, and control access to secure areas. Suggestions have been made that the use of biometrics can potentially increase the security in airports by automatically identifying individual by measuring their physical characteristics, such as fingerprints, iris, retinal, and hand geometry. Concerning convenience, the utilization of biometrics offers travellers the ability to pass through airline check-ins faster, all within the context of enhanced travel security. However, the problems identified with biometrics were privacy concerns which are directly linked to individual's right to privacy.

- **Privacy Concerns**

The four types of privacy concerns identified were information privacy, bodily privacy, privacy of communication, and territorial privacy.

Among the four different types of concerns, information privacy concerns was regarded as the greatest fear due to the inaccuracy of biometrics system, "function creep", centralized data storage, identity theft, illegal disclosure, unauthorised collection, use, and retention of an individual's personal biometrics information.

- With regard to system accuracy, biometric systems will sometimes mistakenly accept an impostor as a valid individual or conversely, reject a valid individual.

- Unauthorised collection creates the risk that personal biometrics information maybe misused.
- Function creep refers to the dangers of finding biometric data exchanged without consent, within the biometric community.
- The easy accessibility of these databases from anywhere in a country has raised fears among civil liberty groups.
- Identity theft is the act of obtaining personal information without the concerned person's consent.
- Unauthorised use - biometric data can be used for purposes broader than those originally intended, including use in tracking.

Privacy is defined as the right individuals have to control what information about them should or should not be communicated to others and under what circumstances. Thus identity theft, "function creep" and the unauthorised use, collection, retention and disclosure of biometrics information impact on an individual's right to privacy.

However, previous research has shown that even if privacy concerns are high and knowledge about biometrics is low, general acceptance of biometrics is by and large high.

7.3.Construct development

A detailed approach towards the investigation of the use of biometrics was the DART-model (Dynamic acceptance model for re-evaluation of technology-based application). The issues surrounding biometrics are privacy, security, attitude towards acceptance, and convenience.

Two dimensions derived from the DART-model that were important for this research were perceived usefulness and perceived cost.

- The dimension "perceived usefulness" deal with aspect of security and convenience.
- The dimension "perceived cost" is related to non material cost (for example, giving up some privacy).

The additional dimension "acceptance of biometrics" comprises the attitude of respondents towards privacy. Three categories of respondents were described in chapter 4:

- The privacy fundamentalist
- The privacy pragmatists
- The privacy unconcerned.

In summary, five dimensions were included in the questionnaire, such as: General Security, Acceptance of biometrics, Privacy Concerns, Protecting Biometric Information, and Balancing Security and Privacy.

Three additional items were included that were measured on a single-item basis, namely: Personal data Collection (item 38), Personal Data Storage (item 37), and Time Taken of Check-in procedure (item 36).

7.4.Empirical study

A questionnaire was developed as a survey instrument. It was created with a 6-point Likert scale, and included an additional "Statement not relevant option" to assess respondents' opinion. The content and structure of a preliminary version was purified by academic personnel from the University of the Western Cape. Their changes and revisions were incorporated into the final questionnaire.

The study population comprised international air travellers residing in the City of Cape Town. In order to avoid bias, a systematic selection of 150 respondents were considered appropriate who are 18 years of age, or older.

The 38-item questionnaire was administered to a pilot group of a systematically selected population. These results were analysed and necessary changes were incorporated into the final version of the questionnaire.

7.5.Statistical analysis

A total of 150 questionnaires were administered with a response rate of 91.3%. The demographic information includes age, gender, occupation, and travel frequencies. The ages of the passengers ranged from 18 years old to above 56 years old, with the majority, that is, 48.5% aged between 26 to 35 years old. With regard to gender, the majority of the respondents were males (68.4%). The t-test was used to test if any significant difference exists between genders and the hypotheses. With respect to occupation, the bulk of respondents were from the working environment (69.1%) followed by students (29.4%). The number of retired was just 1.47% whereas there were no respondents that were unemployment. And finally, the mass of the travellers,

that is, 53.7% travels several times a year followed by 14.7%, 15.4%, and 16.2% who travel "Once a year", "Once a month", and "Once in several years" respectively.

Cronbach's α was used to measure the internal consistency, and one item deleted from the privacy concerns dimension.

There were some items that were used on a single-item basis to get respondents' opinion of current situation at the airport.

- Item 9 (*There is a serious threat that airport terrorist attacks that have occurred in the past, could happen again*), indicated that the bulk of travellers agree that terrorist attack is a grave menace to the society. Due to the poor quality of passenger screening procedures and staffs, respondents believe that terrorists can pass through the security check with little difficulty using falsified travel documents.
- Two items measured travellers' attitude of the airport security. Item 12 and 13 of the survey questionnaire, that is, *I have full confidence in the ability of the passenger screeners to keep air travel secure from hostile individuals* and *Security staff using X-rays screen hand luggage effectively* indicated the seriousness of the current security. This survey has revealed that the majority of passengers agree that security is a serious problem. The survey result proves that the security checkpoint at the airport, which is equipped with X-ray machines for carry-on bags and metal detectors for passengers to walk through, is not considered completely safe.
- Item number 14 (*I am more concerned about safety than my personal rights – for example, I do not object to being searched*) shows that in the

current context people are more concerned about their safety that their personal rights. As a result passengers are willing to pass through various check points of a system where they can be screened by instruments and trained personnel.

- The survey also analysed the behaviour of passengers regarding the extended waiting time at the airport for better security. Item 36 (*It takes longer to do retinal or facial scans or take fingerprints. In the interest of better security at the airport check-in procedure, I would accept*) showed that 67.6% of passengers were keen to spend less than 15 minutes more at the check-in procedure. 11.8% were prepared to spend between 15 minutes and 30 minutes. Only 2.2% were ready to accept more than 30 minutes more, whereas 18.4% had no opinion.

7.6. Conclusion

7.6.1.Results summary of question 1 and the research implication

Question: Will travellers accept biometrics for higher security measures, that is, positive authentication?

Hypothesis: Hypothesis 1 proposed that Biometric security measures at airports are positively accepted by travellers.

The threat of terrorism is a major concern around the world. The security checkpoint at the airport, equipped with X-ray machines and metal detectors is not considered completely safe. Many other factors have been identified that could used by terrorists.

Human error is also inevitable, even in the best of circumstances, due to the repetitive nature of security work, loss of concentration, distraction, and fatigue. As a consequence, ineffective person and luggage screening could contribute to a terrorist attack.

Improving security measures has become an important issue to better protect travellers and airport premises. Biometrics is considered useful tool to strengthen the security at the airports and promises to become ever-present in future at all international airports. Despite the benefit of positive authentication offered by biometrics, there are some challenges associated with it.

Despite the challenges, this research has revealed that South Africans rate biometrics highly. From the sample, 17% replied that they were against biometrics use and 83% of the respondents would accept the use of biometrics to verify their identity at the airport, rather than traditional methods of authentication. The results from this research are very promising and show that safety remains the respondents' top priority.

Statistical analysis showed that 83% of travellers agreed that biometric security measures to be incorporated at the airport. Hypothesis 1 is therefore accepted.

- Finding 1: There was no statistical significant difference between the age groups regarding the acceptance of biometrics for security measures at the airport.

- ❖ Finding 2: There is no significant difference in the attitude between genders regarding the acceptance of biometrics for security measures at the airport.

- ❖ Finding 3: There is no significant difference between the number of times people travel and acceptance of biometrics.

- ❖ Finding 4: There is no significant difference between professional groups regarding the acceptance of biometrics at the airport.

7.6.2. Results summary of question 2 and the research implication

Question: Will passengers be willing to opt for higher security measures by giving up privacy?

Hypothesis: Hypothesis 2 claimed that passengers will sacrifice privacy for higher security.

Privacy is a fundamental human right, one of the most important of the modern age. It underpins human dignity and other key values such as freedom of association and freedom of speech. However, there is growing public concern regarding privacy over the use of biometrics. This research dealt with informational privacy regarding the unlawful use, the unauthorised collection, and the dissemination of personal biometric information. In addition, storage of sensitive biometric information in databases, through extensive data gathering can be accessed from anywhere, thus giving rise to invasions of informational privacy.

Therefore, it is important to understand the use of biometrics that give rise to a number of major informational privacy concerns. These concerns need to be addressed before the public in general is willing to accept the emerging biometrics.

Around the world biometrics has raised privacy concerns. South African travellers' were asked in the survey if they will give up privacy for higher security. 73% agreed to sacrifice their individual right to privacy. They believe that integrating biometrics at the airport would strengthen security and also improve their personal safety.

Even though privacy being an important issue to people, statistical analysis showed that 73% of travellers agreed to give up their right to privacy. Hypothesis 2 is therefore accepted.

- Finding 1: In this research, there appears to be no significant difference between the three groups in connection with sacrificing privacy for higher security. The 3 groups of individuals are prepared to sacrifice their individual's rights to privacy for higher security to strengthen airport safety measures as the statistic shows that $F = 0.186$ ($P>0.05$).

- Finding 2: With regard to sacrificing privacy for higher security, for this research, there exists no significant difference in gender. The data analysis shows that males and females with mean 4.1 and 4.4, and S.D 0.9 respectively resulted in no significant difference as the "t" value is 0.083 ($P>0.05$).

- Finding 3: There was no significant difference (F=0.3, that is, P>0.05) between respondents who travel Once a month (mean=4.0, S.D=1.2), Several times a year (mean=4.4, S.D=0.9), Once a year (mean=4.0, S.D=1.0), and Once in several years (mean=4.2, S.D=0.8) with regard to giving up privacy for advanced security.

- Finding 4: The table shows that there were no significant differences (F=0.198, that is, P>0.05) between the working professional, student, and retired person.

7.6.3. Results summary of question 3 and research implication

Question: Will passengers sacrifice privacy for convenience?

Hypothesis: Hypothesis 3 states that passengers will sacrifice privacy for convenience.

Statistical analysis showed that 92% of travellers would trade privacy for convenience. The above hypothesis is therefore accepted.

Biometrics technology provides enhanced security as well as convenience. An example of convenience for example is the use of biometric technologies at Changi Airport that offers every traveller the dream when it comes to airport procedures: the ability to breeze through airline check-in, security as well as immigration checks in less that one minute, all within the context of enhanced travel security.

The hypothesis focuses on getting an understanding if travellers would surrender their privacy for convenience, even if privacy is a major concern. This survey indicates that the majority of the South Africans were privacy pragmatists. According to (Paine *et al.*, 2005), privacy pragmatists are individuals who are willing allow people to have access to, and the use, their personal information for some benefits, that is, to trade privacy for some convenience.

The majority of respondents, that is, 92%, are willing to sacrifice their privacy for convenience. Therefore hypothesis 3 was accepted as well.

- Finding 1: There was no significant difference between the 3 age groups for sacrificing privacy for convenience.

- Finding 2: The result shows that there was no significant difference between male (mean=5.1, S.D=1.2) and female (mean=5.3, S.D=0.9) about sacrificing privacy for convenience.

- Finding 3: There **was a significant difference** (F=0.032, that is, P<0.05) with regards to air travel frequency and passengers sacrificing privacy for convenience. Respondents travelling "once a month" have mean 4.5 and S.D 1.8 compare to the other groups with mean 5.0 or above and S.D below 1.3, meaning that they are a bit reluctant to give up privacy for convenience.

- ❖ Finding 4: no significant difference (F=0.5) was observed for working professionals (mean=5.1, S.D=1.2), students (mean=5.2, S.D=1.0), and retired (mean=6.0, S.D=0).

In summary, there is no doubt that the use of biometrics is increasing across a wide variety of applications and will expand significantly in the near future. It provides more security and convenience benefits than any other form of authentication technology. This research finds that convenience and security are more important than privacy issues among South Africans. 83% South Africans would be happy to accept biometrics security measures at airports while travelling abroad. 73% would sacrifice their individual rights in favour of higher security for protection against terrorists. 92% of travellers would be happy to use biometrics as they believe this will accelerate the screening and check-in procedure.

7.7. Recommendations for future research

This research has addressed the security and privacy issues surrounding biometrics in the airport context. These issues regarding information privacy include unauthorised collection, use, and retention of biometrics data. The focus of the research investigated the possible use of biometrics at the national level, that is, in the context of South Africa. However, further research is required to understand the issue surrounding biometrics in the international context, for example:

- What are the appropriate measures for ensuring that the disclosure of personal data on an international, multilateral level will not lead to using them for a variety of purposes beyond the original purpose of their collection?

- Who should be entitled to access what information (for example, access control)?
- What safeguards could be put on the initial and secondary uses of the data to verify the compatibility of purposes?
- Should there be specific safeguards for the use of biometric-based data?

As pointed out by the US's Secretary of Homeland Security, biometrics is a tremendous technology to accurately identify and cross-check travellers, however it is important to have a set of international standards for capturing, analyzing, storing, reading, sharing and protection of sensitive information in order to ensure maximum interoperability between systems and maximum privacy for the citizens.

References

Abdelghany, A., Abdelghany, K. and Narasimhan, R. 2006. "Scheduling baggage-handling facilities in congested airports", ***Journal of Air Transport Management***, Vol.12, Iss.2, March 2006, p.76-81.

Adams D.A., Nelson R.R. and Todd P.A. 1992. "Perceived usefulness, ease of use, and usage of information technology: A replication", ***MIS Quarterly***, Vol.16, No.2, p.227-247.

Adey, P. 2004. "Secured and sorted Mobilities: Example from the Airport" [Online], ***Surveillance & Society***, Vol.1, Iss.4, p.500-519, Available from: http://www.surveillance-and-society.org/articles1(4)/sorted.pdf [Accessed: 06 April 2006].

Ahmed, F. and Siyal, M.Y. 2005. "A novel approach for regenerating a private key using password, fingerprint and smart card", ***Information Management & Computer Security***, Vol.13, Iss.1.

Albers, S., Koch, B. and Ruff, C. 2005. "Strategic alliances between airlines and airports-theoretical assessment and practical evidence", ***Journal of Air Transport Management***, Vol.11, Iss.2, March 2005, p.49-58.

Allen, R. 2005. "Biometrics Wields A Double-Edged Sword", ***Electronic Design***, June 2005, Vol.53, iss.14, p.77.

Alterman, A. 2003. "A piece of yourself": Ethical issues in biometric identification", ***Ethics and Information Technology***, Vol.5, Iss.3, ABI/INFORM, p.139.

Amberg, M., Fischer, S. and Schroder, M. 2005. "An evaluation framework for the acceptance of web-based aptitude testa" [Online], ***The Electronic Journal of Information Systems Evaluation***, Vol.8, Iss.3, p.151-158. Available from: www.ejise.com [Accessed: 18 July 2006].

Arndt, C. 2005. "The loss of privacy and identity", ***Biometric Technology Today***, Vol.13, Iss.8, Sep 2005, p.6-7.

Ashbourn, J. 1999. "***The biometric white paper***" [Online], Available from: Http://www.jsoft.freeuk.com/whitepaper.htm [Accessed: 14 February 2006].

Ayoade, J.O. and Kosuge, T. 2002. "Breakthrough in privacy concerns and lawful access conflicts", ***Telematica and Informatics***, Vol.19, Iss.4, November 2002, p.273-289.

Banisar, D. 2002. "***Privacy and Human Rights 2002, An international Survey of privacy Laws and Development***", [Online], First Edition 2002, Printed in the United States of America, Electronic Privacy Information Centre and Privacy International. Available from: [Accessed: 28 March 2006].

Belanger, F., Hiller, J.S. and Smith, W.J. 2002. "Trustworthiness in electronice commerce: the role of privacy, security, and site attributes", ***Journal of Strategic Information Systems***, Vol.11, p.245-270.

Bennett, P. 2000. "***Access control by audio-visual recognition***", Vol.49, Iss.1.

Bente, G., Surakka, V., Lylykangas, J., Vuorinen, K., Troitzsch, H., Eschenburg, F. and Krämer, N. 2005. "***Deliverable D6.3: Report on results of first phase usability testing and guidelines for developers***" [Online], BioSec, Available from: www.europeanbiometrics.info/images/resources [Accessed: 18 July 2006].

Bente, G., Surakka, V., Lylykangas, J., Vuorinen, K., Troitzsch, H., Eschenburg, F. and Krämer, N. 2005. "***Deliverable D6.5: Introduction of a Multi-Modular Acceptance and Usability Questionnaire***" [Online], BioSec, Available from: www.europeanbiometrics.info/images/resources/72_186_file.pdf [Accessed: 18 July 2006].

Black, G.S. 2005. "Is eBay for everyone: an assessment of consumer demographics", ***SAM Advanced Management Journal***, Vol.79, p.50-59.

Bolle, R.M., Connell, J.H. and Ratha, N. 2002. "Biometric perils and patches", ***Pattern Recognition***, Vol.35, Iss.12, December 2002, p.2727-2738.

Braggins, D. 2001. "Fingerprint sensing and analysis", ***Sensor Review***, Bradford, Vol.21, Iss.4, p.272.

Brown, M. and Muchira, R. 2004. "Investigating the relationship between internet privacy concerns and online purchase behaviour", ***Journal of Electronic Commerce Research***, Vol.5, No.1.

Brown, M.L. and Kros, J.F. 2003. "Data mining and the impact of missing data", ***Industrial Management & Data Analysis***, Vol.103, No.8, p.611-621.

Caelli, W., Longley, D. and Shain, M. 1994. ***Information Security Handbook***, Paperback Edition, Macmillan Press Ltd, Great Britain.

Calvert, P. and Pope, A. 2005. "Telephone survey research for library managers", ***Library Management***, Vol.26, No.3, 2005.

Campadelli, P., Lanzarotti, R. and Savazzi, C. 2003. "***A Feature-Based Face Recognition System***", 12th International Conference on Image Analysis and Processing (ICIAP' 03), September 2003, p.68.

Carblanc, A. and Bernat, L. 2004. "Background material on biometrics and enhanced network systems for the security of international travel" [Online], ***Information Security and Privacy***. Available from: http://www.oecd.org/sti/security-privacy [Accessed: 04 October 2006].

Casal, C.R. 2004. "Impact of location-aware services on the privacy/security balance", ***Info***, Vol.6, No.2, pp.105-111.

Cavoukian, A. 1999a. "***Biometrics and Policing: Comment from a Privacy Perspective***" [Online], information and privacy commissioner/Ontario, Available from http://www.ipc.on.ca/userfiles/page_attachments/biometric.pdf [Accessed: 08 June 2006].

Cavoukian, A. 1999b. "***Consumer Biometric Applications: A Discussion Paper***" [Online], information and privacy commissioner/Ontario, Available from: http://www.ipc.on.ca/userfiles/page_attachments/cons-bio.pdf [Accessed: 08 June 2006].

Chan, S.L. 2000. "Information technology in business processes", ***Business Process Management Journal***, Vol.6, No.3, p.224-237.

Chauvel, D. and Despres, C. 2002. "A review of survey research in knowledge management", ***Journal of Knowledge Management***, Vol.6, Iss.3.

Clarke, R. 1999. "Internet privacy concerns confirm the case for intervention", Association for Computing Machinery. Commission of the ACM; Feb 1999, Vol.42, Iss.2, ***ABI/INFORM Global***, p.60.

Chen, G. and Astebro, T. 2003. "How to deal with missing categorical data: Test of a simple Bayesian Method", ***Organisational Research Methods***, Vol.6, No.3, July 2003, p.300-327.

Connie, T., Teoh, A., Goh, M. and Ngo, D. 2004. "PalmHashing: a novel approach for cancellable biometrics", ***Information Processing Letter*** 93, 2005, p.1-5.

Connolly, C. 2006. "Image processing algorithms underpinning iris and facial recognition systems", ***Sensor Review***, Vol.26, Iss.1.

Coughlin, C.C., Cohen, P. and Khan, S.R. 2002. "***Aviation Security and Terrorism: A Review of Economic Issues***", September/October 2002.

Crawshaw, J. and Chambers, J. 1994. "***A concise course in A-level statistics***", Third edition, Stanley Thorns (Publishers) Ltd. Great Britain.

D' Ambra, J. and Wilson, C.S. 2004. "Explaining perceived performance of the World Wide Web: Uncertainty and the task-technology fit model", ***Internet Research***; Vol.14, Iss.4.

Davis, F.D. 1989. "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology," ***MIS Quarterly***, Vol.13, No.3, p319-340.

Davis, R. 2005. "Giving body to biometrics", ***The British Journal of Administrative Management***, Apr/May 2005, iss.46, p.32-33.

Davis, S.G. 1994. "Touching Big Brother: How biometric Technology Will Fuse Flesh and Machine", ***Information Technology & People***, Vol.7, Iss.4, p.38-47.

Davis, S. 1999. "Biometrics – A civil liberties and privacy perspective", ***Information Security Technical Report***, Vol.4, Supplement.1, 1999, p.32

Deshpande, S., Chikkerur, S. and Govindaraju, V. 2005. "***Accent Classification in Speech***", Fourth IEEE workshop on Automatic Identification Advanced Technologies (AutoID' 05).

Desmarais, N. 2000. "Body language, security and e-commerce", ***Library Hi Tech***, Vol.18, Iss.1.

Dlamini, N. 2005. "***Police already preparing for 2010***" [Online], Available from: http://www.southafrica.info/2010/saps2010.htm [Accessed: 02 Feb 2006].

Doggett, T. 2002. "Forget privacy, give us biometrics!", ***Biometric Technology Today***, July/August, Vol.10, iss.7.

Dority, B. 2001. "A brave new world—or a technology nightmare? Big brother is watching!", ***The Humanist***, May/June 2001, Vol.61, Iss.3, p.9.

Dumortier, J. and Kindt, E. 2005. "***Biometrics and Security: Summary of legal data protection requirements for the processing of biometric data (based on D.4.2 of BioSec)***" [Online]. Available from: http://www.europeanbiometrics.info/search/index.php [Accessed: 08 June 2006].

Elizabeth, M. 2000. "***Qualitative research methods in health technology assessment: a review of the literature***" [Online], Available from: http://www.refer.nhs.uk/viewrecord.asp?id=87 [Accessed: 14 October 2006].

Elliott, L., Nerney, M., Jones, T. and Friedmann, P.D. 2002. "Barriers to screening for domestic violence" [Online], ***Journal of General Internal Medicine***, Vol.17, Iss.2, p.112-116. Available from: http://www.pubmedcentral.nih.gov/articlerender.fcgi?artid=1495014 [Accessed: 15 October 2006].

Forza, C. 2002. "Survey research in operations management: a process-based perspective", ***International Journal of Operations & Production Management***, Vol.22, No.2, p.152-194.

Friedewald, M., Vildjiounaite, E., Punie, Y. and Wright, D. 2006. "Privacy, identity and security in ambient intelligence: A scenario analysis", ***Telematics and Informatics***, In Press, 13 January 2006.

Gelbord, B. and Roelofsen, G. 2002. "New surveillance techniques raise privacy concerns", Association for computing machinery. ***Communications of the ACM***. New York. Nov 2002, Vol.45, Iss.11, p.23.

Giesing, I. 2003. "The identification of user perceptions related to identification through biometrics within electronic business" [Online], ***Masters' Thesis***, University

of Pretoria, South Africa. Available from: http://upetd.up.ac.za/thesis/available [Accessed: 03 September 2006]

Gilbert, D., Lee-Kelley, L. and Barton, M. 2003. "Technophobia, gender influences and consumer decision-making for technology-related products", ***European Journal of Innovation Management***, Vol. 6, No.4, p.253-263.

Gilbert, D. and Wong, R.K.C. 2003. "Passenger expectations and airline services: a Hong Kong based study", ***Tourism Management***, Vol.24, Iss.5, October 2003, p.519-532.

Gopal, R., Garfinkel, R., Nunez, M. and Rice, D. 2006. "***Electronic Markets for private information: economic and security considerations***", Proceedings of the 39th annual Hawaii international conference on system sciences (HICSS'06) Track 6, January 2006, p.113a.

Graeff, T.R. and Harmon, S. 2002. "Collecting and using personal data: consumers' awareness and concerns", ***Journal of consumer marketing***, Vol.19, Iss.4, p.302-318.

Grijpink, J. 2001. "Privacy Law: Biometrics and privacy", ***Computer Law & Security Report***, Vol.17, Iss.3, 1 May 2001, p.154-160.

Heracleous, L. and Wirtz, J. 2006. "Biometrics: the next frontier in service excellence, productivity and security in the service sector", ***Managing Service Quality***, Vol.16, No.1, p.12-22.

http://www.concourt.org.za [Accessed: 24/08/2005]

International Biometric Group, 2000-2005. "***IBG's Biometric Privacy Impact Assessment***" [Online],
Available from: http://www.bioprivacy.org/index.htm [Accessed: 03 April 2006].

Jackson, C.M., Chow, S. and Leitch, R.A. 1997. "Towards an understanding of the behavioural intention to use an information system", ***Decision Science***, Spring 1997, Vol.28, Iss.2, p.357.

Jain, A., Hong, L. and Pankanti, S. 2000. "Biometric identification", ***Association for computing machinery, Communication of the ACM***, February 2000, Vol.43, Iss.2, p.90.

Janes, J. 1999. "Survey Construction", ***Library Hi Tech***, Vol.17, Iss.3.

Janes, J. 1999. **"Why a column on research techniques?"**, ***Library Hi Tech***, Vol.17, Iss.2.

Joinson, A.N. and Paine, C.B. 2006. "***Self-disclosure, Privacy and the Internet***" [Online], Available from:
http://www.york.ac.uk/res/e-society/projects/15/PRISD_report2.pdf [Accessed: 09 September 2006].

Juels, A., Molnar, D. and Wagner, D. 2005. "***Security and Privacy Issues in E-passports***", [Online], Available from: http://mirror.cr.yp.to/eprint.iacr.org/2005/095.pdf [Accessed: 06 April 2006]

Karjoth, G. and Schunter, M. 2002. "A privacy policy model for enterprises", 15th ***IEEE Computer Security Foundations Workshop*** (CSFW' 02), June, p.271.

Kitchenham, B. and Pfleeger, S.L. 2003. "Principles of Survey Research Part 6: Data Analysis", ***Software Engineering Notes***, Vol.28, no.2.

Kivela, J., Reece, J. and Inbakaran, R. 1999. "***Consumer research in the restaurant environment. Part 2: Research design and analytical methods***", International Journal of Contemporary Hospitality Management, Vol.11, Iss.6.

Kochan, A. 2004. "Breakthrough in Biometrics", ***Sensor Review***, 2004, Vol.24, Iss.2.

Kolodinsky, J.M., Hogarth, J.M. and Hilgert, M.A. 2004. "The adoption of electronic commerce banking technologies by US consumers", ***The International Journal of Bank Marketing***, Vol.22, No.4, p.238-259.

Kondrasuk, J.N. 2004. "The effects of 9/11 and terrorism on human resources management: Recovery, Reconsideration, and Renewal", ***Employee Responsibilities and Rights Journal***, Vol.16, No.1, March 2004.

Kondrasuk, J.N. 2005. "A US view of terrorism", ***Disaster Prevention and Management***, Vol.14, Iss.5, 2005.

Koneya, M. 1977. "Privacy regulation in small and large groups", ***Group & organisation studies*** (pre-1986); Sep 1977, Vol.2, Iss.3, p.324.

Kress, K., Ozawa, N. and Schmid, G. 2000. "The new consumer emerges", ***Strategy & Leadership***, Vol.28, Iss.2.

Kroeker, K.L. 2002. "Graphic and Security: Exploring Visual Biometrics", ***IEEE Computer Graphics and Applications***, Vol.22, Iss.4, July/August 2002.

Kumar, S., Sim, T., Janakiraman, R. and Zhang, S. 2005. "***Using Continuous Biometric Verification to Protect Interactive Login Sessions***", 21st Annual Computer Security Application Conference (ACSAC' 05), December 2005, p.441-450.

Kuzz, E.R. and Colapinto, R. 2003. "Privacy rules", ***CA magazine***, Nov 2003, Vol.136, Iss.9.

Langenderfer, J. and Linnhoff, S. 2005. "The Emergence of Biometrics and its Effects on Consumers", ***Journal of Consumer Affairs***, Winter 2005, Vol.39, iss.2, p.314.

Legris, P., Ingham, J. and Collerette, P. 2001. "Why do people use information technology? A critical review of the technology acceptance model", ***Information & Management***, Vol.40, p.191-204.

Leone, K. and Liu, R.R. 2005. "The key design parameters of checked baggage security screening systems in airports", ***Journal of Air Transport Management***, Vol.11, Iss.2, p.69-78.

Lewis, Curt, L., Montgomery, and John, F. 1989. "Air travel safety/security for the business person", ***Professional safety***, Vol.34, Iss.6, June 1989, p.44.

Lin, N. 1976. "***Foundations of Social Research***", Mc Graw-Hill Book Company, Printed in the United States of America.

Liu, C. and Arnett, K.P. 1999. "Exploring the factors associated with Web site success in the context of electronic commerce", ***Information & Management***, Vol.38, p.23-33.

Liu, X., Bowyer, K.W. and Flynn, P.J. 2005. "Experimental Evaluation of Iris Recognition", 2005 ***IEEE Computer Society Conference on computer vision and Pattern Recognition (CVPR' 05)***, June, p.158.

Loring, T.B. 2002. "An analysis of the informational privacy protection afforded by the European Union and the United States", ***Texas International Law Journal***, Spring 2002, Vol.37, Iss.2, p.421.

Lu, J., Yu, C.S., Liu, C. and Yao, J.E. 2003. "Technology acceptance model for wireless Internet", ***Internet Research: Electronic Networking Applications and Policy***, Vol.13, No.3, p.206-222.

Lui, S. and Silverman, M. 2001. "A Practical Guide to Biometric Security Technology", ***IT Professional***, January 2001, p.27-32.

Lyon, D. 2002. "Everyday Surveillance: Personal data and social classifications", ***Information, Communication & Society***, Apr, Vol.5, iss.2, p.242.

Ma, Q. and Liu, L. 2004. "The Technology Acceptance Model: A Meta-Analysis of Empirical Findings", ***Journal of Organisational and End User Computing***, Jan-Mar 2004, Vol.16, Iss.1, p.56.

Mansfield, G.M. 2005. "A strategic architecture and its role in enhancing the performance of commercial web-enabled enterprises" [Online], ***PhD Thesis***, University of Stellenbosch, Cape Town, South Africa,
Available from: http://www.strategyinstitute.co.za/ [Accessed: 15 March 2006].

Mascarenhas, O.A.J., Kesavan, R. and Bernacchi, M.D. 2003. "Co-managing online privacy a call for joint ownership", ***Journal of consumer marketing***, Vol.20, No.7, p.686-702.

Matyas, V. and Riha, Z. 2003. "Toward Reliable User Authentication through Biometrics", ***IEEE Security and Privacy***, p.45-49.

McClelland, S.M. 1994. "Training Needs Assessment Data-gathering Methods: Part 1, Survey Questionnaires", ***Journal of European Industrial Training***; Vol.18, Iss.1.

Mc Cullagh, K. 2005. "***Identity information: the tension between privacy and the societal benefits associated with biometric database surveillance***", Paper presented to 20th BILETA Conference: Over-Commoditised; Over-Centralised; Over-Observed: New Digital Legal World?, Queen's University of Belfast, April, p.1-14.

McMullan, R. 2005. "A multiple item scale for measuring customer loyalty development", ***Journal of Services Marketing***, Vol.19, Iss.7.

Metzger, M.J. 2004. "Privacy, Trust, and Disclosure: Exploring Barriers to Electronic Commerce" [Online], Vol.9, No.4, July 2004, Available from: http://jcmc.indiana.edu/vol9/issue4/metzger.html [Accessed:12 September 2006].

Mladen, C. 2002. "Privacy in Canada: A Report of Research on Privacy for Electronic Government" [Online], Available from: http://joi.ito.com/privacyreport/Contents_Distilled/EnglishSection/Canada_E_p252-314.pdf [Accessed: 03 April 2006].

Moore, T. 2003. "IBG's Look at Biometric and Privacy Issues" [Online], International ***Biometric Group***, IDNewswire, Vol.2, No.17. Available from: http://criterianlabs.org/media/82003IDNewswire.pdf [Accessed: 26 September 2006]

Most, C.M. 2004. "Towards Privacy Enhancing Applications of Biometrics", [Online], Available from: http://www.europeanbiometrics.info/images/resources/32_219_file.pdf [Accessed: 08 June 2006]

Munich, M.E. and Perona, P. 2003. "Visual identification by signature Tracking", ***IEEE Transactions on Pattern Analysis and Machine Intelligence***, February 2003, p.200-217.

ORC International. 2001 – 2002. "Public Attitudes towards the Uses of Biometric Identification Technologies by Government and the Private Sector" [Online], Available from: http://www.search.org/files/pdf/Biometricsurveyfindings.pdf [Access:16 November 2005].

Özel, B., Çilingir, C.B. and Erkan, K. 2006. "Towards Open Source Software Adoption: Educational, Public, Legal, and Usability Practices" [Online], Available from: www.tossad.org/content/download/1195/6084/file/oss_2006_tossad_workshop_proceedings.pdf [Accessed: 18 July 2006].

Paine, C., Joinson, A.N., Buchanan, T. and Reips, U. 2005. "Watch me, watching you: Privacy attitudes and reactions to identity card implementation scenarios in the United States", ***Journal of Information System***. [Online], Available from: http://www.york.ac.uk/res/e-society/projects/15/Joinson_et_al_06.pdf [Access: 23 May 2006].

Pentland, A.S. and Choudhury, T. 2000. "Face recognition for smart environment", ***Computer***, Feb, p.50-55.

Pirie, G. 2006. "'Africanisation' of South Africa's international air links", ***Journal of Transport Geography***, Vol.14, Iss.1, January, p.3-14.

Porter, M.E. 1985. "Competitive advantage" [Online], chapter 1, pp.11-15, The Free Press. New York. Available from: http://www.ifm.eng.cam.ac.uk/dstools/paradigm/valuch.html [Accessed: 02 February 2006]

Postnote. 2001. "Biometrics & technology" [Online], Available from: www.parliament.uk/post/home.htm [Accessed: 05 August 2005]

Prabhakar, S., Pankanti, S. and Jain, A.K. 2003. "Biometric Recognition: Security and Privacy Concerns", ***IEEE Security and Privacy***, March, p.33-42.

Pun, K.H. and Moon, Y.S. 2004. "Recent Advances in Ear Biometrics", Sixth IEEE International Conference on Automatic Face and Gesture Recognition, May 2004, p.164.

Randall, D. 2005. "Disruptive scenarios. Four futures: privacy battles and chatty networks", Vol.33, No.3, p.47-49.

Ratha, N.K., Connell, J.H. and Bolle, R.M. 2001. "Enhancing security and privacy in biometrics-based authentication systems", ***IBM Systems Journal***, 2001, Vol.40, iss.3, p.614.

Rhee, T.H., Cho, S.J. and Kim, J.H. 2001. "On-line signature verification using Model-guided Segmentation and Discriminative Feature Selection for Skilled Forgeries", ***Sixth International Conference on Document Analysis and Recognition (ICDAR' 01)***, September, p.0645.

Rhodes, K.A. 2003. "Information Security: Challenge in Using Biometrics" [Online], United States General Accounting Office. Available from: http://www.gao.gov/new.items/d031137t.pdf [Accessed:13 September 2006]

Ridge, T. 2005. Available from: http://www.dhs.gov/dhspublic/display?content=4304 [Accessed: 04 October 2006]

Roger, A. 2005. "Biometrics wields a double-edge sword", ***Electronic Design***, Vol.53, Iss.14, p.77-81.

Ross, A. and Jain, A. 2003. "Information Fusion in Biometrics", ***Pattern Recognition Letter***, Vol.24, Iss.13, p.2115-2125, Sep.

Scherer, K. 2005. "Biometrics: Past, Present and Future", ***Futurics***, Vol.29, Iss.3/4; Academic Research Library, p.83.

Schreiner, K. 1999. "Iris recognition", ***IEEE Intelligent Systems***, November 1999, p.2-7.

Schimmel, K. and Nicholls, J. 2003. "***Gender Differences and E-commerce Behaviour and Perceptions***" [Online], Vol. 8, No.1,
Available from: http://www.arraydev.com/commerce/JIBC/0303-01.htm [Accesses: 12 September 2006].

Sekaran, U. 2000. "***Research Methods for Business: A skill-building Approach***." USA: John Wiley & Sons Inc. p.125

Sheehan, K.B. 2002. "Towards a Typology of Internet Users and Online Privacy Concerns", ***The Information Society***, Vol.18, Iss.1, p.21-32.

Sierles, F.S. 2003. "How to do research with self-administered surveys" [Online], ***Academic Psychiatry***, Vol.27, Iss.2, summer 2003, Available from: http://www.ap.psychiatryonline.org/cgi/reprint/27/2/104 [Accessed: 02 May 2006]

Sims, D. 1994. "Decriminalizing the Fingerprint", ***IEEE Computer Graphics and Applications***, July 1994, p.15-16

Singh, S. and Singh, M. 2003. "Explosives detection system (EDS) for aviation security", ***Signal Processing***, Vol. 83, p.31-55.

Slemrod, J. 2006. "Taxation and Big Brother: Information, Personalisation and Privacy in the 21st century Tax Policy", ***Fiscal studies***, Vol.27, no.1, p.1-15, March.

Smith, J.M. 1972. "***Interviewing in market and social research***", Routledge & Kegan Paul Ltd, London.

Stephanie, S., Linderholm, O. and Moore, C. 2001. "Privacy concerns raised", ***InfoWorld***, September 17, 2001, Vol.23, Iss.38, p.24.

Stephen, P. and Hornby, S. 1995. "The joys of statistics", ***Library Review***, Vol.44, Iss.8.

Steyn, L. 2004. "Human rights issues in South African insolvency law", International ***Insolvency Review***, Spring 2004, Vol.13, iss.1, p.3.

Stibbe, M. 2005. "Flight paths to security", ***Infosecurity Today***, Vol.2, Iss.5, September-October 2005, p.33-35.

Taipale, K.A. 2004/2005. "Technology, Security and Privacy: The fear of Frankenstein, The Mythology of Privacy and the Lessons of King Ludd", ***International Journal of Communication Law & Policy***, Special Issue on Cybercrime, Iss.9.

Tavani, H.T. 1999. "Informational privacy, data mining, and the Internet", ***Ethics and Information Technology***, Vol.1, Iss.2, p.137.

Teng, M. 2005. "***The impact of security on E-Biz in a Global Economy***" [Online], Informatics Institute. H@cker Halted.
Available from: http://www.informatics.com.mx [Accessed: 30 August 2006].

Thomas, R.A.L. 2005. "Biometrics, international migrants and human rights" [Online], ***Global Migration Perspectives***, January 2005, No 17, Available from: http://www.gcim.org/gmp/Global%20Migration%20Perspectives%20No%2017.pdf [Accessed: 06 April 2006].

Torbet, G.E., Marshall, I.M. and Jones, S. 1995. "One in the eye to plastic card fraud", ***International Journal of Retail & Distribution Management***, Vol.23, Iss.5.

Torrez, E., Dominguez, J.S., Valdez, L. and Aza, R. 2005. "Passenger Waiting Time in an Airport and Expenditure carried out in the Commercial area", ***Journal of Air Transport Management***, Vol.11, Iss.6, November, p.363-367.

Turney, M.A., Bishop, J.C. and Fitzgerald, P.C. 2004. "Measuring the importance of recent airport security interventions", ***Journal of Air Transportation***, Vol.9, Iss.3, p.56.

Tyson, J. and Grabianowski, E.D. 2002. "***How Airport Security Works***" [online], Available from: http://travel.howstuffworks.com/airport-security9.htm [13 February 2006].

Tzannatos, E.S. 2003. "A decision support system for the promotion of security in shipping", ***Disaster Prevention and Management***, Vol.12.

Udo, G.J. 2001. "Privacy and security concerns as major barriers for e-commerce: a survey study", ***Information Management & Computer Security***, Vol.9, Iss.4, p.165-174.

Vaughan-Nichols, S.J. 2004. "Voice authentication Speaks to the Marketplace", ***Computer***, March 2004, p.13-15.

Venkatesh, V. and Davis, F.D. 2000. "A theoretical extension of the technology acceptance model: Four longitudinal field studies", ***Management Science***, February 2000, Vol.46, Iss.2, p.186.

Viaene, J. 1997. "Consumer behaviour towards light products in Belgium", ***British Food Journal***; Vol.99, Iss.3.

Wah, C.C. and Feng, H. 2002. "Private Key Generation From on-line Handwritten Signature", ***Information Management & Computer Security***, Vol.10, Iss.4.

Wahler, P. and Tully, C.J. 1991. "Young People's Attitude to Technology", ***European Journal of Education***, Vol.26, No.3, p.261-272.

Whisenant, W.A. 2003. "Using biometrics for sport venue management in a post 9-11 era", ***Facilities***, Vol.21, No.5/6, p.134-141.

Wikipedia. 2005. Free encyclopaedia [Online] Available from: http://en.wikipedia.org/wiki/Privacy [Accessed: 20/10/2005]

Wikipedia. 2006. "Quantitative research" [Online], Available from: http://en.wikipedia.org/wiki/Quantitative_research [Accessed: 14 October 2006]

Williams, P. and Gunter, B. 2006. "Triangulating qualitative research and computer transaction logs in health information studies", ***Aslib Proceedings***, Vol.58, Iss.1/2.

Woodcock, A. 2005. "Biometric cards: privacy invaders vs. a safer America", ***Computers and Society***, Vol.35, Iss.1, March, p.3.

Wright, T. 1994. "Privacy and Electronic Identification in the Information Age" [Online], Available from: http://www.ipc.on.ca/ [Accessed: 13 September 2006].

Weisberg, H.F. and Bowen, B.D. 1977. "An introduction to survey research and data analysis", Printed in the United States of America.

Whisenant, W.A. 2003. "Using biometrics for sport venue management in a post 9-11 era", ***Facilities***; Vol.21, Iss.5/6.

Wright, D. 2005. "The dark side of ambient intelligence", Vol.7, Iss.6, p.33-51.

Yamazaki, Y., Mizutani, Y. and Komatsu, N. 1999. "Extraction of Personal Fatures from Stroke Shape, Writing Pressure and Pen Inclination in Ordinary Characters", ***Fifth International Conference on Document Analysis and Recognition (ICDAR' 99)***, September 1999, p.426.

Yan, P. and Bowyer, K.W. 2005. "Empirical Evaluation of Advanced Ear Biometrics", ***IEEE Computer society conference on computer vision and Pattern Recognition (CVPR' 05)***, June 2005, p.41.

Yang, Z., Jun, M. and Peterson, R.T. 2004. "Measuring customer perceived online service quality: Scale development and managerial implications", ***International Journal of Operations & Production Management***, Vol.24, No.11, p.1149-1174

Yoo, K.E. and Choi, Y.C. 2005. "Analytic hierarchy process approach for identifying relative importance of factors to improve passenger security checks at airports", ***Journal of Air Transport Management***, Vol.12, p.135-142.

Zhang, Y., Kundu S.J., Goldgof, D.B., Sarkar, S. and Tsap, L.V. 2004. "Elastic Face, An Anatomy-Based Biometrics Beyond Visible Cue", ***17th International Conference on Pattern Recognition (ICPR' 04)***, Vol.2, p.19-22.

Zorkadis, V. and Donos, P. 2004. "On biometrics-based authentication and identification from a privacy-protection perspective: Deriving privacy-enhancing requirements", ***Information Management & Computer Security***, Vol.12, Iss.1.

APPENDICES

APPENDIX 1: Questionnaire

Dear Traveller,
As part of a Masters research project, the University of the Western Cape (UWC) is conducting an academic survey of passenger regarding airport security and the personal right to privacy. The survey takes about 10 minutes to complete. UWC guarantee confidentiality. Your cooperation is greatly appreciated. **Dr Glen Mansfield Tel 083 282 8410**

Demographic information

1. Surname (Optional) .....
2. Address (Optional) .....
3. Age (In years) .....

Please tick the appropriate box

4. Gender Male □ Female □
5. Air travel frequency Once a month □ Several times a year □ Once a year □ Once in years
6. Purpose of your travel Business □ Visiting □ Holidays □ Study
7. Occupation Working Professional □ Student □ Unemployed □ Retired
8. Which of the following are you familiar with?

	I have given a fingerprint before	□
AND/OR	Retinal scan	□
AND/OR	Iris scan	□
AND/OR	Hand Geometry scan	□
AND/OR	Facial Recognition	□

NONE of the above ☐

Please tick only one check-box for each statement below	Totally Disagree (1)	Mostly Disagree (2)	Some-times Disagree (3)	Some-times Agree (4)	Mostly Agree (5)	Totally Agree (6)	Statement not relevant
9. There is a serious threat that airport terrorist attacks that have occurred in the past, could happen again	☐	☐	☐	☐	☐	☐	☐
10. The airline industry is liable (has a legal responsibility) for protecting passengers from terrorist attacks	☐	☐	☐	☐	☐	☐	☐
11. All airline and airport personnel should be screened to ensure they have no criminal record	☐	☐	☐	☐	☐	☐	☐
12. I have full confidence in the ability of the passenger screeners to keep air travel secure from hostile individuals	☐	☐	☐	☐	☐	☐	☐
13. Security staff using X-rays screen hand-luggage effectively	☐	☐	☐	☐	☐	☐	☐
14. I am more concerned about safety than my personal rights - for example, I do not object to being searched	☐	☐	☐	☐	☐	☐	☐
15. I would allow retinal or facial scans or fingerprints to be taken if it makes the airports safer	☐	☐	☐	☐	☐	☐	☐
16. A retinal or facial scan or fingerprints would also ensure a higher security level than using PIN numbers when making a secure transaction on a computer	☐	☐	☐	☐	☐	☐	☐
17. I would use retinal or facial scans or fingerprints rather than passwords when working on a computer or ATM	☐	☐	☐	☐	☐	☐	☐
18. I generally accept the use of devices and systems that do retinal or facial scans or take fingerprints	☐	☐	☐	☐	☐	☐	☐
19. I would have confidence in devices and systems that do retinal	☐	☐	☐	☐	☐	☐	☐

or facial scans or take fingerprints

Please tick only one check-box for each statement below	Totally Disagree (1)	Mostly Disagree (2)	Some-times Disagree (3)	Some-times Agree (4)	Mostly Agree (5)	Totally Agree (6)	Statement not relevant
20. I would approve the use of retinal or facial scan or fingerprints if they increase my own security, for example, assist in the prevention of terrorist attacks	□	□	□	□	□	□	□
21. I would approve the use of retinal or facial scan or fingerprints if they increase the security of other passengers	□	□	□	□	□	□	□
22. A flight in which the identity of the passengers is confirmed with retinal or facial scan or fingerprints is likely to be safer than one secured using a traditional passport photograph	□	□	□	□	□	□	□
23. I would accept using retinal or facial scan or fingerprints if they accelerated the check-in procedure	□	□	□	□	□	□	□
24. I am prepared to give up some rights to privacy if it will prevent terrorist attacks	□	□	□	□	□	□	□
25. I am prepared to give up some rights to privacy if it will prevent theft and fraud	□	□	□	□	□	□	□
26. There is a possibility that my stored personal security data could be misused for unscrupulous use	□	□	□	□	□	□	□
27. I am confident that my stored personal security data (for example, retinal or facial scan or fingerprint) cannot be stolen	□	□	□	□	□	□	□
28. The registration of my personal security data (for example, retinal or facial scan or fingerprint) is generally likely to lead to high levels of surveillance and loss of personal privacy	□	□	□	□	□	□	□
29. I am concerned that facial recognition could be used to track every move I make	□	□	□	□	□	□	□

Please tick only one check-box for each statement below	Totally Disagree (1)	Mostly Disagree (2)	Some-times Disagree (3)	Some-times Agree (4)	Mostly Agree (5)	Totally Agree (6)	Statement not relevant
30. The airline industry should not use passengers' data obtained from retinal or facial scan or fingerprints for any other purposes than originally described	□	□	□	□	□	□	□
31. Passengers must have an avenue of redress if their personal security data is violated	□	□	□	□	□	□	□
32. Airline industry collecting passengers' data will keep the data secure from unauthorised access	□	□	□	□	□	□	□
33. Airline industry will inform passengers before putting their personal security data to other use	□	□	□	□	□	□	□
34. Airline industry collecting passengers' data will do so accurately	□	□	□	□	□	□	□
35. Devices and systems that do retinal or facial scans or take fingerprints take time. I would accept the application of such systems at check-in time for the benefits of better security	□	□	□	□	□	□	□

36. It takes longer to do retinal or facial scans or take fingerprints. In the interest of better security at the airport check-in procedure, I would accept:

- Less than 15 minutes more □
- 15 minutes - 30 minutes more □
- More than 30 minutes more □
- No preference □

37. Personal data from retinal or facial scans or fingerprints must be stored somewhere. I would prefer to:

Hold my data personally (for example, on a smart card)	☐
Have my data held in a central repository managed by (say) the Airports Company [of South Africa]	☐
I have no opinion	☐

38. Personal data needs to be collected. To whom would I be happy to give permission to collect and hold data on my retinal or facial scans or fingerprints:

The government and official institutions	☐
Employers	☐
Hospitals and health centres	☐
Data security firms	☐
Commercial organisations	☐
Other (Specify)	.....
NONE	☐

Thank You Very Much!

APPENDIX 2: Tables (Replacing missing values)

Frequencies (Item 3 - 7)
Demographic Profile

APPENDIX 3: Statistics (Demographic Profile)

		Age	Gender	Air travel frequency	Purpose of your travel	Occupation
N	Valid	136	136	136	136	136
	Missing	0	0	0	0	0

Frequency Table

APPENDIX 4: Age

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	18 - 25 years	30	22.1	22.1	22.1
	26 - 35 years	66	48.5	48.5	70.6
	36 - 45 years	25	18.4	18.4	89.0
	46 - 55 years	12	8.8	8.8	97.8
	56 years and above	3	2.2	2.2	100.0
	Total	136	100.0	100.0	

APPENDIX 5: Gender

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Male	93	68.4	68.4	68.4
	Female	43	31.6	31.6	100.0
	Total	136	100.0	100.0	

APPENDIX 6: Air travel frequency

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Once a month	21	15.4	15.4	15.4
	Several times a year	73	53.7	53.7	69.1
	Once a year	20	14.7	14.7	83.8
	Once in several years	22	16.2	16.2	100.0
	Total	136	100.0	100.0	

APPENDIX 7: Purpose of your travel

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Business	25	18.4	18.4	18.4
	Visiting	66	48.5	48.5	66.9
	Holidays	31	22.8	22.8	89.7
	Study	14	10.3	10.3	100.0
	Total	136	100.0	100.0	

Frequencies (Items 9 - 35)
General Security
Privacy Concerns
Acceptance of Biometrics
Protecting Biometrics Information

Statistics (9-15)

		Item 9	Item 10	Item 11	Item 12	Item 13	Item 14	Item 15
N	Valid	136	136	136	136	136	136	136
	Missing	0	0	0	0	0	0	0

Statistics (16-22)

		Item 16	Item 17	Item 18	Item 19	Item 20	Item 21	Item 22
N	Valid	136	136	136	136	136	136	136
	Missing	0	0	0	0	0	0	0

Statistics (23-29)

		Item 23	Item 24	Item 25	Item 26	Item 27	Item 28	Item 29
N	Valid	136	136	136	136	136	136	136
	Missing	0	0	0	0	0	0	0

Statistics (30-35)

		Item 30	Item 31	Item 32	Item 33	Item 34	Item 35
N	Valid	136	136	136	136	136	136
	Missing	0	0	0	0	0	0

Frequency Table

APPENDIX 8: Occupation

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Working professional	94	69.1	69.1	69.1
	Student	40	29.4	29.4	98.5
	Retired	2	1.5	1.5	100.0
	Total	136	100.0	100.0	

APPENDIX 9: Frequency tables after replacing missing values with mean and mode

Item 9

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Totally Disagree	6	4.4	4.4	4.4
	Mostly Disagree	7	5.1	5.1	9.6
	Sometimes Disagree	13	9.6	9.6	19.1
	Sometimes Agree	34	25.0	25.0	44.1
	Mostly Agree	25	18.4	18.4	62.5
	Totally Agree	51	37.5	37.5	100.0
	Total	136	100.0	100.0	

Item 10

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Totally Disagree	7	5.1	5.1	5.1
	Mostly Disagree	6	4.4	4.4	9.6
	Sometimes Disagree	8	5.9	5.9	15.4
	Sometimes Agree	13	9.6	9.6	25.0
	Mostly Agree	24	17.6	17.6	42.6
	Totally Agree	78	57.4	57.4	100.0
	Total	136	100.0	100.0	

Item 11

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Totally Disagree	7	5.1	5.1	5.1
	Mostly Disagree	5	3.7	3.7	8.8
	Sometimes Disagree	5	3.7	3.7	12.5
	Sometimes Agree	9	6.6	6.6	19.1
	Mostly Agree	16	11.8	11.8	30.9
	Totally Agree	94	69.1	69.1	100.0
	Total	136	100.0	100.0	

Item 12

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Totally Disagree	13	9.6	9.6	9.6
	Mostly Disagree	12	8.8	8.8	18.4
	Sometimes Disagree	23	16.9	16.9	35.3
	Sometimes Agree	43	31.6	31.6	66.9
	Mostly Agree	25	18.4	18.4	85.3
	Totally Agree	20	14.7	14.7	100.0
	Total	136	100.0	100.0	

Item 13

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Totally Disagree	4	2.9	2.9	2.9
	Mostly Disagree	13	9.6	9.6	12.5
	Sometimes Disagree	15	11.0	11.0	23.5
	Sometimes Agree	27	19.9	19.9	43.4
	Mostly Agree	46	33.8	33.8	77.2
	Totally Agree	31	22.8	22.8	100.0
	Total	136	100.0	100.0	

Item 14

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Totally Disagree	6	4.4	4.4	4.4
	Mostly Disagree	6	4.4	4.4	8.8
	Sometimes Disagree	10	7.4	7.4	16.2
	Sometimes Agree	16	11.8	11.8	27.9
	Mostly Agree	26	19.1	19.1	47.1
	Totally Agree	72	52.9	52.9	100.0
	Total	136	100.0	100.0	

Item 15

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Totally Disagree	8	5.9	5.9	5.9
	Mostly Disagree	3	2.2	2.2	8.1
	Sometimes Disagree	9	6.6	6.6	14.7
	Sometimes Agree	19	14.0	14.0	28.7
	Mostly Agree	18	13.2	13.2	41.9
	Totally Agree	79	58.1	58.1	100.0
	Total	136	100.0	100.0	

Item 16

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Totally Disagree	10	7.4	7.4	7.4
	Mostly Disagree	6	4.4	4.4	11.8
	Sometimes Disagree	16	11.8	11.8	23.5
	Sometimes Agree	18	13.2	13.2	36.8
	Mostly Agree	27	19.9	19.9	56.6
	Totally Agree	59	43.4	43.4	100.0
	Total	136	100.0	100.0	

Item 17

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Totally Disagree	15	11.0	11.0	11.0
	Mostly Disagree	9	6.6	6.6	17.6
	Sometimes Disagree	8	5.9	5.9	23.5
	Sometimes Agree	16	11.8	11.8	35.3
	Mostly Agree	28	20.6	20.6	55.9
	Totally Agree	60	44.1	44.1	100.0
	Total	136	100.0	100.0	

Item 18

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Totally Disagree	5	3.7	3.7	3.7
	Mostly Disagree	8	5.9	5.9	9.6
	Sometimes Disagree	6	4.4	4.4	14.0
	Sometimes Agree	25	18.4	18.4	32.4
	Mostly Agree	37	27.2	27.2	59.6
	Totally Agree	55	40.4	40.4	100.0
	Total	136	100.0	100.0	

Item 19

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Totally Disagree	5	3.7	3.7	3.7
	Mostly Disagree	4	2.9	2.9	6.6
	Sometimes Disagree	15	11.0	11.0	17.6
	Sometimes Agree	26	19.1	19.1	36.8
	Mostly Agree	40	29.4	29.4	66.2
	Totally Agree	46	33.8	33.8	100.0
	Total	136	100.0	100.0	

Item 20

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Totally Disagree	4	2.9	2.9	2.9
	Mostly Disagree	4	2.9	2.9	5.9
	Sometimes Disagree	4	2.9	2.9	8.8
	Sometimes Agree	16	11.8	11.8	20.6
	Mostly Agree	35	25.7	25.7	46.3
	Totally Agree	73	53.7	53.7	100.0
	Total	136	100.0	100.0	

Item 21

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Totally Disagree	4	2.9	2.9	2.9
	Mostly Disagree	3	2.2	2.2	5.1
	Sometimes Disagree	4	2.9	2.9	8.1
	Sometimes Agree	16	11.8	11.8	19.9
	Mostly Agree	34	25.0	25.0	44.9
	Totally Agree	75	55.1	55.1	100.0
	Total	136	100.0	100.0	

Item 22

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Totally Disagree	5	3.7	3.7	3.7
	Mostly Disagree	4	2.9	2.9	6.6
	Sometimes Disagree	8	5.9	5.9	12.5
	Sometimes Agree	15	11.0	11.0	23.5
	Mostly Agree	43	31.6	31.6	55.1
	Totally Agree	61	44.9	44.9	100.0
	Total	136	100.0	100.0	

Item 23

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Totally Disagree	4	2.9	2.9	2.9
	Mostly Disagree	3	2.2	2.2	5.1
	Sometimes Disagree	4	2.9	2.9	8.1
	Sometimes Agree	13	9.6	9.6	17.6
	Mostly Agree	41	30.1	30.1	47.8
	Totally Agree	71	52.2	52.2	100.0
	Total	136	100.0	100.0	

Item 24

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Totally Disagree	15	11.0	11.0	11.0
	Mostly Disagree	6	4.4	4.4	15.4
	Sometimes Disagree	11	8.1	8.1	23.5
	Sometimes Agree	27	19.9	19.9	43.4
	Mostly Agree	31	22.8	22.8	66.2
	Totally Agree	46	33.8	33.8	100.0
	Total	136	100.0	100.0	

Item 25

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Totally Disagree	11	8.1	8.1	8.1
	Mostly Disagree	6	4.4	4.4	12.5
	Sometimes Disagree	14	10.3	10.3	22.8
	Sometimes Agree	28	20.6	20.6	43.4
	Mostly Agree	35	25.7	25.7	69.1
	Totally Agree	42	30.9	30.9	100.0
	Total	136	100.0	100.0	

Item 26

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Totally Disagree	5	3.7	3.7	3.7
	Mostly Disagree	2	1.5	1.5	5.1
	Sometimes Disagree	8	5.9	5.9	11.0
	Sometimes Agree	31	22.8	22.8	33.8
	Mostly Agree	30	22.1	22.1	55.9
	Totally Agree	60	44.1	44.1	100.0
	Total	136	100.0	100.0	

Item 27

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Totally Disagree	20	14.7	14.7	14.7
	Mostly Disagree	22	16.2	16.2	30.9
	Sometimes Disagree	24	17.6	17.6	48.5
	Sometimes Agree	29	21.3	21.3	69.9
	Mostly Agree	21	15.4	15.4	85.3
	Totally Agree	20	14.7	14.7	100.0
	Total	136	100.0	100.0	

Item 28

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Totally Disagree	8	5.9	5.9	5.9
	Mostly Disagree	13	9.6	9.6	15.4
	Sometimes Disagree	13	9.6	9.6	25.0
	Sometimes Agree	30	22.1	22.1	47.1
	Mostly Agree	42	30.9	30.9	77.9
	Totally Agree	30	22.1	22.1	100.0
	Total	136	100.0	100.0	

Item 29

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Totally Disagree	13	9.6	9.6	9.6
	Mostly Disagree	10	7.4	7.4	16.9
	Sometimes Disagree	16	11.8	11.8	28.7
	Sometimes Agree	42	30.9	30.9	59.6
	Mostly Agree	25	18.4	18.4	77.9
	Totally Agree	30	22.1	22.1	100.0
	Total	136	100.0	100.0	

Item 30

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Totally Disagree	2	1.5	1.5	1.5
	Mostly Disagree	5	3.7	3.7	5.1
	Sometimes Disagree	4	2.9	2.9	8.1
	Sometimes Agree	7	5.1	5.1	13.2
	Mostly Agree	20	14.7	14.7	27.9
	Totally Agree	98	72.1	72.1	100.0
	Total	136	100.0	100.0	

Item 31

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Mostly Disagree	1	.7	.7	.7
	Sometimes Disagree	3	2.2	2.2	2.9
	Sometimes Agree	6	4.4	4.4	7.4
	Mostly Agree	18	13.2	13.2	20.6
	Totally Agree	108	79.4	79.4	100.0
	Total	136	100.0	100.0	

Item 32

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Totally Disagree	5	3.7	3.7	3.7
	Mostly Disagree	7	5.1	5.1	8.8
	Sometimes Disagree	16	11.8	11.8	20.6
	Sometimes Agree	21	15.4	15.4	36.0
	Mostly Agree	29	21.3	21.3	57.4
	Totally Agree	58	42.6	42.6	100.0
	Total	136	100.0	100.0	

Item 33

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Totally Disagree	10	7.4	7.4	7.4
	Mostly Disagree	10	7.4	7.4	14.7
	Sometimes Disagree	14	10.3	10.3	25.0
	Sometimes Agree	13	9.6	9.6	34.6
	Mostly Agree	22	16.2	16.2	50.7
	Totally Agree	67	49.3	49.3	100.0
	Total	136	100.0	100.0	

Item 34

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Totally Disagree	7	5.1	5.1	5.1
	Mostly Disagree	7	5.1	5.1	10.3
	Sometimes Disagree	19	14.0	14.0	24.3
	Sometimes Agree	24	17.6	17.6	41.9
	Mostly Agree	32	23.5	23.5	65.4
	Totally Agree	47	34.6	34.6	100.0
	Total	136	100.0	100.0	

Item 35

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Totally Disagree	6	4.4	4.4	4.4
	Mostly Disagree	6	4.4	4.4	8.8
	Sometimes Disagree	5	3.7	3.7	12.5
	Sometimes Agree	31	22.8	22.8	35.3
	Mostly Agree	40	29.4	29.4	64.7
	Totally Agree	48	35.3	35.3	100.0
	Total	136	100.0	100.0	

Frequencies (Item 36 - 38)
Additional Items

Statistics

		Item 36	Item 37	Item 38
N	Valid	136	136	136
	Missing	0	0	0

Frequency Table

Item 36

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Less than 15 minutes more	92	67.6	67.6	67.6
	15 minutes - 30 minutes more	16	11.8	11.8	79.4
	More than 30 minutes more	3	2.2	2.2	81.6
	No Preference	25	18.4	18.4	100.0
	Total	136	100.0	100.0	

Item 37

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Hold my data personally (for example, on a smart card)	88	64.7	64.7	64.7
	Have my data held in a sentral repository managed by ACSA	27	19.9	19.9	84.6
	I have no opinion	21	15.4	15.4	100.0
	Total	136	100.0	100.0	

Item 38

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Government and Official Institutions	53	39.0	39.0	39.0
	Employers	3	2.2	2.2	41.2
	Hospitals and Health Centres	13	9.6	9.6	50.7
	Data Security Firms	31	22.8	22.8	73.5
	None	36	26.5	26.5	100.0
	Total	136	100.0	100.0	

APPENDIX 10: Reliability Test

Reliability test

Dimension 1:

Case Processing Summary

		N	%
Cases	Valid	136	100.0
	Excluded(a)	0	.0
	Total	136	100.0

a Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	N of Items
.849	9

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
Item 15	38.11	58.277	.603	.829
Item 16	38.48	55.348	.682	.819
Item 17	38.55	54.486	.644	.825
Item 18	38.31	62.111	.462	.843
Item 19	38.43	60.454	.570	.832
Item 20	37.96	58.021	.772	.815
Item 21	37.93	58.839	.743	.818
Item 22	38.13	61.242	.545	.835
Item 29	39.04	66.665	.195	.872

Dimension 2:

Case Processing Summary

		N	%
Cases	Valid	136	100.0
	Excluded(a)	0	.0
	Total	136	100.0

a Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	N of Items
.594	6

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
Item 24	21.88	15.127	.656	.380
Item 25	21.85	16.532	.591	.426
Item 26	21.38	24.475	.006	.658
Item 27	22.78	20.514	.203	.607
Item 28	22.00	20.800	.244	.584
Item 35	21.54	20.472	.325	.552

Second reliability test of Dimension 2:

Case Processing Summary

		N	%
Cases	Valid	136	100.0
	Excluded(a)	0	.0
	Total	136	100.0

a Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	N of Items
.658	5

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
Item 24	16.98	13.888	.647	.479
Item 25	16.94	15.359	.569	.529
Item 27	17.88	17.340	.329	.647
Item 28	17.10	19.939	.184	.701
Item 35	16.64	18.484	.367	.626

APPENDIX 11: Age

Frequency

Age

Statistics

age2

N	Valid	136
	Missing	0

age2

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1.00	96	70.6	70.6	70.6
	2.00	37	27.2	27.2	97.8
	3.00	3	2.2	2.2	100.0
	Total	136	100.0	100.0	

ANOVA

		6XP RI 6TXDUHV	GI	0 HDQ6TXDUH	)	6IJ
P HDQ	%HWZHHQ* URXSV	1.726	2	.863	.945	.391
	: LWKLQ* URXSV	121.436	133	.913		
	7RWDO	123.162	135			
P HDQ	%HWZHHQ* URXSV	3.301	2	1.650	1.703	.186
	: LWKLQ* URXSV	128.864	133	.969		
	7RWDO	132.165	135			
P HDQ	%HWZHHQ* URXSV	2.679	2	1.340	.970	.382
	: LWKLQ* URXSV	183.725	133	1.381		
	7RWDO	186.404	135			

APPENDIX 12: Gender

Group Statistics

	* HQGHU	1	0 HDQ	6WG ' HYLDWLRQ	6WG (UURU 0 HDQ
P HDQ	0 DOH	93	4.7145	.99494	.10317
	) HP DOH	43	4.9561	.85040	.12969
P HDQ	0 DOH	93	4.1763	.99601	.10328
	) HP DOH	43	4.4930	.95054	.14496
P HDQ	0 DOH	93	5.1290	1.27028	.13172
	) HP DOH	43	5.3023	.93948	.14327

ANOVA

		6XP RI 6TXDUHV	GI	0 HDQ6TXDUH	)	6LJ
P HDQ	%HWZHHQ* URXSV	5.623	3	1.874	2.105	.103
	: LWKLQ* URXSV	117.539	132	.890		
	7RWDO	123.162	135			
P HDQ	%HWZHHQ* URXSV	3.120	3	1.040	1.064	.367
	: LWKLQ* URXSV	129.045	132	.978		
	7RWDO	132.165	135			
P HDQ	%HWZHHQ* URXSV	12.008	3	4.003	3.030	.032
	: LWKLQ* URXSV	174.396	132	1.321		
	7RWDO	186.404	135			

APPENDIX 13: Occupation

Descriptives

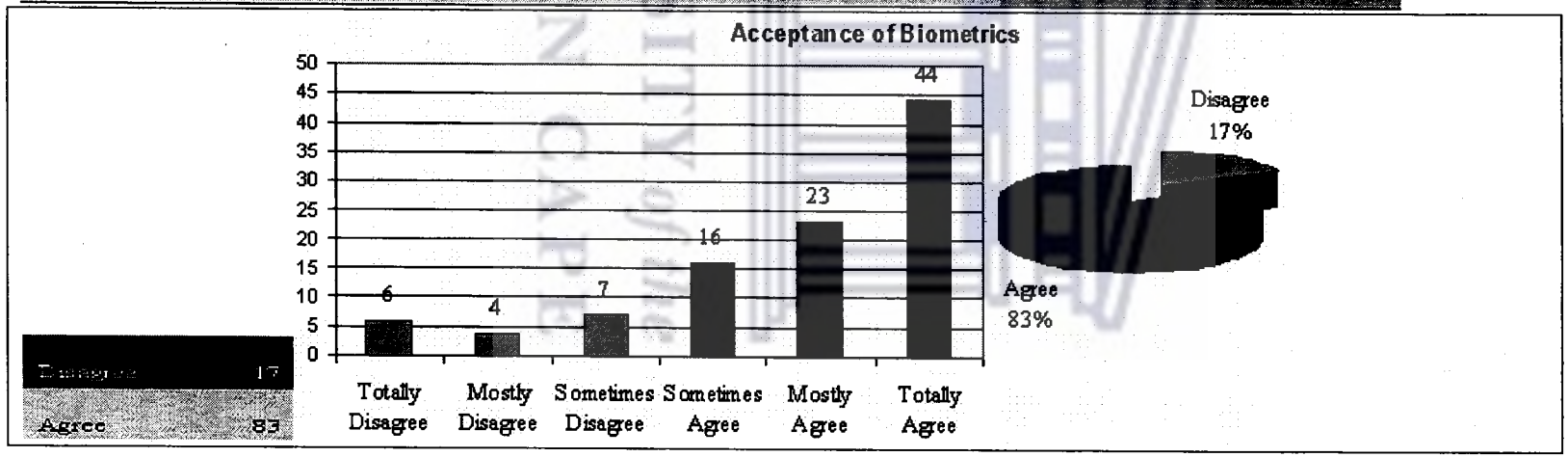
		N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
						Lower Bound	Upper Bound		
mean1	Working professional	94	4.7742	.98204	.10129	4.5731	4.9754	1.00	6.00
	Student	40	4.8056	.91857	.14524	4.5118	5.0993	2.33	6.00
	Retired	2	5.2778	.23570	.16667	3.1601	7.3955	5.11	5.44
	Total	136	4.7908	.95515	.08190	4.6289	4.9528	1.00	6.00
mean2	Working professional	94	4.3191	.98169	.10125	4.1181	4.5202	1.00	6.00
	Student	40	4.1250	1.00224	.15847	3.8045	4.4455	1.40	5.60
	Retired	2	5.3000	.42426	.30000	1.4881	9.1119	5.00	5.60
	Total	136	4.2765	.98944	.08484	4.1087	4.4443	1.00	6.00
mean3	Working professional	94	5.1489	1.24397	.12831	4.8941	5.4037	1.00	6.00
	Student	40	5.2250	1.02501	.16207	4.8972	5.5528	2.00	6.00
	Retired	2	6.0000	.00000	.00000	6.0000	6.0000	6.00	6.00
	Total	136	5.1838	1.17506	.10076	4.9845	5.3831	1.00	6.00

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
mean1	Between Groups	.509	2	.254	.276	.759
	Within Groups	122.653	133	.922		
	Total	123.162	135			
mean2	Between Groups	3.184	2	1.592	1.642	.198
	Within Groups	128.981	133	.970		
	Total	132.165	135			
mean3	Between Groups	1.515	2	.757	.545	.581
	Within Groups	184.890	133	1.390		
	Total	186.404	135			

APPENDIX 14: Hypothesis 1

Acceptance of Biometrics by Travellers												
	Item 15	Item 16	Item 17	Item 18	Item 19	Item 20	Item 21	Item 22	Item 29	Total (x)	(x/7 x)*100	To the nearest dp
Totally Disagree	8	10	13	5	5	4	4	5	13			
Mostly Disagree	3	6	9	8	4	4	3	4	10			
Sometimes Disagree	9	16	8	6	15	4	4	8	16			
Sometimes Agree	19	18	16	25	26	16	16	15	42			
Mostly Agree	18	27	28	37	40	35	34	43	25			
Totally Agree	79	59	60	55	46	73	75	61	30			



Age	Mean	Standard Deviation	Number of Respondents	F# (ANOVA test)	P-value
Group 1	4.7477	0.86930	96	0.391	P > 0.05
Group 2	4.8468	1.17073	37		
Group 3	5.4815	0.39021	3		

APPENDIX 15: Age (Acceptance of Biometrics)

Gender	Mean	Standard Deviation	Number of Respondents	F-value	P-value
Male	4.7145	0.99494	93	0.171	P > 0.05
Female	4.9561	0.85040	43		

APPENDIX 16: Gender (Acceptance of Biometrics)

Air Travel Frequency	Mean 1	Standard Deviation	Number of Respondents	ANOVA	P-value
Once a month	4.3810	1.30742	21	0.103	P > 0.05
Several times a year	4.9239	0.85704	73		
Once a year	4.6222	0.91724	20		
Once in several years	4.8939	0.83040	22		

APPENDIX 17: Air Travel Frequency (Acceptance of Biometrics)

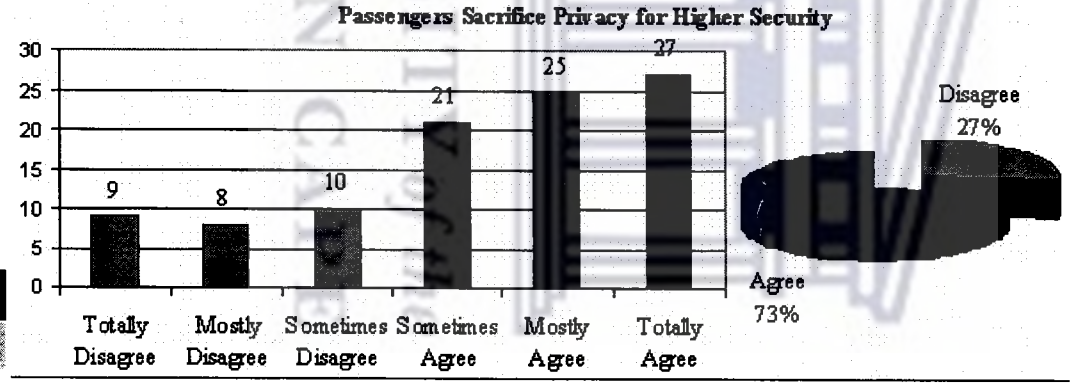
Occupation	Mean 1	Standard Deviation	Number of respondents	ANOVA	P-value
Working Professional	4.7742	0.98204	94	0.759	P > 0.05
Student	4.8056	0.91867	40		
Retired	5.2778	0.23570	2		

APPENDIX 18: Occupation (Acceptance of Biometrics)

APPENDIX 19: Hypothesis 2

Passengers Sacrifice Privacy for Higher Security								
	Item 24	Item 25	Item 27	Item 28	Item 35	Total (x)	(x/?x)*100	To nearest d.p
Totally Disagree	15	11	20	8	6			
Mostly Disagree	6	6	22	13	6			
Sometimes Disagree	11	14	24	13	5			
Sometimes Agree	27	28	29	30	31			
Mostly Agree	31	35	21	42	40			
Totally Agree	46	42	20	30	48			
							100	

Disagree	27
Agree	73



Age	Mean 2	Standard Deviation	Number of Respondents	ANOVA test	P value
Group 1	4.2250	1.00116	96	0.186	P > 0.05
Group 2	4.3297	0.96404	37		
Group 3	5.2667	0.30551	3		

APPENDIX 20: Age (Sacrifice Privacy for Higher Security)

Gender	Mean 2	Standard Deviation	Number of Respondents	P value	P value
Male	4.1763	0.99601	93	0.083	P > 0.05
Female	4.4930	.95054	43		

APPENDIX 21: Gender (Sacrifice Privacy for Higher Security)

Air Travel Frequency	Mean 2	Standard Deviation	Number of Respondents	ANOVA	P value
Once a month	4.0952	1.23874	21	0.367	P > 0.05
Several times a year	4.4000	0.91287	73		
Once a year	4.0200	1.06207	20		
Once in several years	4.2727	0.89771	22		

APPENDIX 22: Air Travel Frequency (Sacrifice Privacy for Higher Security)

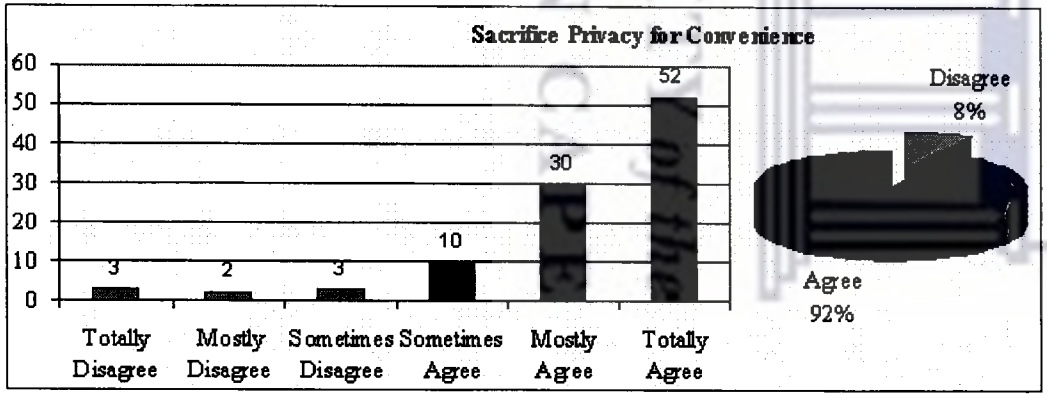
Occupation	Mean 2	Standard Deviation	Number of respondents	ANOVA	P value
Working Professional	4.3191	0.98169	94	0.198	P > 0.05
Student	4.1250	1.00224	40		
Retired	5.3000	0.42426	2		

APPENDIX 23: Occupation (Sacrifice Privacy for Higher Security)

APPENDIX 24: Hypothesis 3

Passengers Sacrifice Privacy for Convenience	
Totally Disagree	3
Mostly Disagree	2
Sometimes Disagree	3
Sometimes Agree	10
Mostly Agree	30
Totally Agree	52

Disagree	8
Agree	92



Age	Means	Standard Deviation	Number of Respondents	F (ANOVA test)	P value
Group 1	5.2083	1.04546	96	0.382	P > 0.05
Group 2	5.0541	1.48970	37		
Group 3	6.0000	0.00000	3		

APPENDIX 25: Age (Sacrifice Privacy for Convenience)

Gender	Means	Standard deviation	Number of respondents	F value	P value
Male	5.1290	1.27028	93	0.426	P > 0.05
Female	5.3023	0.93948	43		

APPENDIX 26: Gender (Sacrifice Privacy for Convenience)

Air travel frequency	Means	Standard Deviation	Number of Respondents	ANOVA	P value
Once a month	4.5714	1.80476	21	0.032	P < 0.05
Several times a year	5.3151	0.95564	73		
Once a year	5.0000	1.29777	20		
Once in several years	5.5000	0.74001	22		

APPENDIX 27: Air Travel Frequency (Sacrifice Privacy for Convenience)

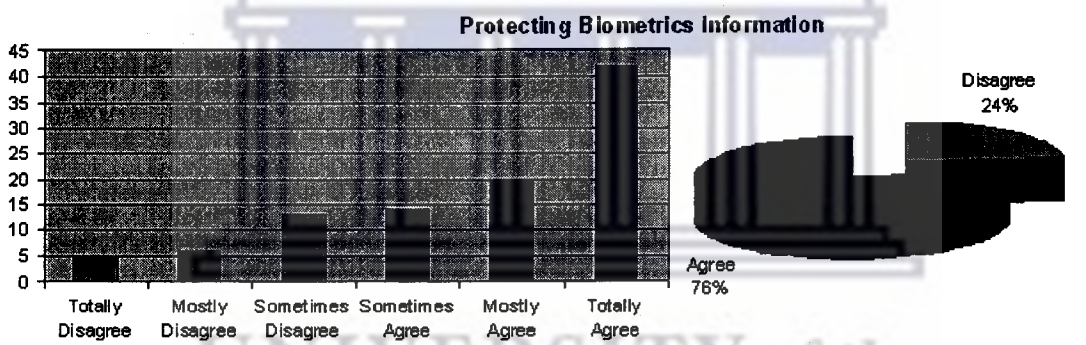
Occupation	Means	Standard Deviation	Number of respondents	ANOVA	P value
Working Professional	5.1489	1.24397	94	0.581	P > 0.05
Student	5.2250	1.02501	40		
Retired	6.0000	0.0000	2		

APPENDIX 28: Occupation (Sacrifice Privacy for Convenience)

APPENDIX 29: Protecting Biometrics Information

Protecting Biometrics Information						
	Item 32	Item 33	Item 33	Total (x)	(x/∑x)*100	To nearest d.p
Totally Disagree	5	10	7	22	5.3921569	5
Mostly Disagree	7	10	7	24	5.8823529	6
Sometimes Disagree	16	14	19	49	12.009804	13
Sometimes Agree	21	13	24	58	14.215686	14
Mostly Agree	29	22	32	83	20.343137	20
Totally Agree	58	67	47	172	42.156863	42
				408	100	100

Disagree	24
Agree	76



Exercise 2

Mission Statement

The University of the Western Cape is a national university, alert to its African and international context as it strives to be a place of quality, a place to grow. It is committed to excellence in teaching, learning and research, to nurturing the cultural diversity of South Africa, and to responding in critical and creative ways to the needs of a society in transition. Drawing on its proud experience in the liberation struggle, the university is aware of a distinctive academic role in helping build an equitable and dynamic society. In particular it aims to:

- advance and protect the independence of the academic enterprise.
- design curricular and research programmes appropriate to its southern African context.
- further global perspectives among its staff and students, thereby strengthening intellectual life and contributing to South Africa's reintegration in the world community.
- assist educationally disadvantaged students gain access to higher education and succeed in their studies.
- nurture and use the abilities of all in the university community.
- develop effective structures and conventions of governance, which are democratic, transparent and accountable.
- seek racial and gender equality and contribute to helping the historically marginalised participate fully in the life of the nation.
- encourage and provide opportunities for lifelong learning through programmes and courses.
- help conserve and explore the environmental and cultural resources of the southern African region, and to encourage a wide awareness of these resources in the community.
- co-operate fully with other stakeholders to develop an excellent, and therefore transformed, higher education system.

Goals

1) Improve the quality of teaching to increase our output
2) Produce competent students
3) Improve our image in society
4) Be in good standing with government policies
5) Be financially viable

Objectives

1) Improve gender equality within a year.
2) Increase our student output by 20% in 2008
3) Improve debt collection from 50% to 90% by 2009
4) …

CSF

1) Improve gender equality within a year.
    a. Admit equal number of male and female students
    b. Keep track of numbers and inform the community
2) Increase our student output by 20% in 2008
    a. Improve quality of lecturing
    b. Measure the quality of lecturing yearly

3) Improve debt collection from 50% to 90% by 2009
    a. Send regular reminders to debtors as per arrangements
    b. Have report on payments as per arrangements

IS Strategy (how will IT help achieve CSF)

1) Improve gender equality within a year.
    a. Admit equal number of male and female students

    Include a Male/Female (Gender) field in the application form.

    b. Keep track of numbers and inform the community

    Create a UWC Gender Equality Web Portal and extract data reports about gender statistics at UWC and allow people to comment online

    or

    a. Provide training support to females on compass (students and staff)

    On the UWC Gender portal, create online tutorials on different gender related topics including Women in the Work Place, Women in Leadership, etc.

    b. keep track of male/female related complaints

    Have a system that will allow logging of gender related complaints both online and physically.

2) Increase our student output by 20% in 2008
    a. Improve quality of lecturing

    Provide online support for lecturers with tutorials on different teacher training topics

    b. Measure the quality of lecturing yearly

    Create a portal where students will be able to rate the quality of lecturing on a regular basis e.g. per month or

3) Improve debt collection from 50% to 90% by 2009
    a. Send regular reminders to debtors as per arrangements

    Develop a system that will be integrated with the current finance system to remind debtors who default on a monthly basis.

    b. Keep track of payment and follow up on a monthly basis and have report on payments as per arrangements

    Produce monthly reports from the system stated above on defaulting debtors.

Exercise 3 Sample Solution

IS 311 (140 340)
Date issued: 21 February 2007

Q1: Give examples of how attacking companies can use IT to **increase** the impact of the five forces in Porters' model within the Retail industry.

Sample Solution:

This is a new companies/new an entrant who wants to penetrate the market. Therefore the question is how they can best penetrate the impact of these forces in order to be part of the Retail industry.

Barrier to New Entrant: This new entrant is a force on its own. Just by using the internet to take its business online already creates an awareness of a new product and service that is comparable with other in the market based on the information access to customers (have the option to match their information/product requirements with the most appropriate means of supply) and the extent of its customer service.

Bargaining power of Supplier: The new entrant can approach the current suppliers within the existing distribution and supply chain management system and offer them direct access to their products and customers. IT can assist in the sense that it will link up the supplier system with the retailing system which will aid in better product forecasting for the supplier and better customer service in terms of delivery schedules.

Bargaining power of Buyer/Customer: Use IT to allow customer to not only view product information but the opportunity to search for the best possible price, through the use of intelligent systems.

Substitute products and or services: Use IT to provide an additional after care service, such as online tailoring. Allowing the customer the opportunity to tailor the product to their fit.

Rivalry amongst competition: Use IT to compete differently by cutting out the middleman and bringing the supply chain to the customers (online vertical/horizontal exchange market/e-market) and linking the customer current and future requirements to the supply chain. This essentially changes the way of competition.

Q2:

Within the Retail sector give examples that show how IT can help the defending company **reduce** the impact of the five forces in Porter's model.

Sample Solution:

This is an existing company within the retail industry and who wants to defend its stance in the market. Therefore the question is how they can best use the impact of these forces to eliminate possible new entries into their market.

Barrier to New Entrant: Use IT to better control the distribution chain better, through providing customers with product tracking and traceability and better market segment analysis in order to personalize direct marketing from the supplier side.

Bargaining power of Supplier: Use IT to better understand the market requirements as to how and when they want it. Through CRM, Sales forecasting and Market segment analysis. Reducing cost in terms of inventory holding space, production and possible rejection of product or service.

Bargaining power of Buyer/Customer: Use IT to lock in customers by providing online financial assistance.

Substitute products and or services: Use IT to study and anticipate competitors move in order for the defending company to take the timed-dependent opportunity.

Rivalry amongst competition: Use IT to redefine market segments/niche markets and better refine products and service to tailor the needs to the various market segments/niches. This makes it very difficult for a new entrant to enter a highly classified market.

Exercise 3 Sample Solution

IS 311 (140 340)
Date issued: 21 February 2007

Q1: Give examples of how attacking companies can use IT to **increase** the impact of the five forces in Porters' model within the Retail industry.

Sample Solution:

This is a new companies/new an entrant who wants to penetrate the market. Therefore the question is how they can best penetrate the impact of these forces in order to be part of the Retail industry.

Barrier to New Entrant: This new entrant is a force on its own. Just by using the internet to take its business online already creates an awareness of a new product and service that is comparable with other in the market based on the information access to customers (have the option to match their information/product requirements with the most appropriate means of supply) and the extent of its customer service.

Bargaining power of Supplier: The new entrant can approach the current suppliers within the existing distribution and supply chain management system and offer them direct access to their products and customers. IT can assist in the sense that it will link up the supplier system with the retailing system which will aid in better product forecasting for the supplier and better customer service in terms of delivery schedules.

Bargaining power of Buyer/Customer: Use IT to allow customer to not only view product information but the opportunity to search for the best possible price, through the use of intelligent systems.

Substitute products and or services: Use IT to provide an additional after care service, such as online tailoring. Allowing the customer the opportunity to tailor the product to their fit.

Rivalry amongst competition: Use IT to compete differently by cutting out the middleman and bringing the supply chain to the customers (online vertical/horizontal exchange market/e-market) and linking the customer current and future requirements to the supply chain. This essentially changes the way of competition.

Q2:

Within the Retail sector give examples that show how IT can help the defending company **reduce** the impact of the five forces in Porter's model.

Sample Solution:

This is an existing company within the retail industry and who wants to defend its stance in the market. Therefore the question is how they can best use the impact of these forces to eliminate possible new entries into their market.

Barrier to New Entrant: Use IT to better control the distribution chain better, through providing customers with product tracking and traceability and better market segment analysis in order to personalize direct marketing from the supplier side.

Bargaining power of Supplier: Use IT to better understand the market requirements as to how and when they want it. Through CRM, Sales forecasting and Market segment analysis. Reducing cost in terms of inventory holding space, production and possible rejection of product or service.

Bargaining power of Buyer/Customer: Use IT to lock in customers by providing online financial assistance.

Substitute products and or services: Use IT to study and anticipate competitors move in order for the defending company to take the timed-dependent opportunity.

Rivalry amongst competition: Use IT to redefine market segments/niche markets and better refine products and service to tailor the needs to the various market segments/niches. This makes it very difficult for a new entrant to enter a highly classified market.