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

By

Ganeshwar Kumar Bhunjun

***

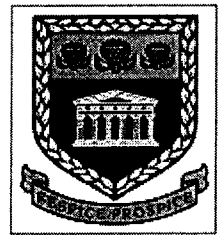
A thesis submitted in fulfilment of the requirements for the Degree of

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;