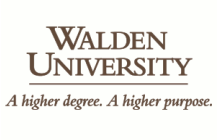


1-1-2011

Biometrics Technology: Understanding Dynamics Influencing Adoption for Control of Identification Deception Within Nigeria

Gideon U. Nwatu
Walden University

Walden University

COLLEGE OF MANAGEMENT AND TECHNOLOGY

This is to certify that the doctoral dissertation by

Gideon U. Nwatu

has been found to be complete and satisfactory in all respects,
and that any and all revisions required by
the review committee have been made.

Review Committee
Dr. Raghu Korrapati, Committee Chairperson,
Applied Management and Decision Sciences Faculty

Dr. Stephanie Lyncheski, Committee Member,
Applied Management and Decision Sciences Faculty

Dr. Walter McCollum, University Reviewer
Applied Management and Decision Sciences Faculty

Chief Academic Officer

David Clinefelter, Ph.D.

Walden University
2011

Abstract

One of the objectives of any government is the establishment of an effective solution to significantly control crime. Identity fraud in Nigeria has generated global attention and negative publicity toward its citizens. The research problem addressed in this study was the lack of understanding of the dynamics that influenced the adoption and usability of biometrics technology for reliable identification and authentication to control identity deception. The support for this study was found in the theoretical framework of the technology acceptance model (TAM). The purpose of the study was to provide scholarly research about the factors that influenced the adoption of biometrics technology to reliably identify and verify individuals in Nigeria to control identity fraud. The mixed-method descriptive and inferential study used interview and survey questionnaires for data collection. The binary logistic regression, point bi-serial correlation, independent samples *t* test, and content analyses were performed using SPSS version 18, Microsoft Excel spreadsheet 2007, and Nvivo 7.0 software. The results from the findings indicated statistical correlation between *adopt biometrics technology* and three other variables, *ease of use* ($r = .38$, $n = 120$, $p < .01$), *perceived usefulness* ($r = .41$, $n = 120$, $p < .01$), and *awareness* ($r = .33$, $n = 120$, $p < .01$). The implications for social change include leveraging biometrics technology for recognition, confirmation, and accountability of individuals to prevent identity scheming, ensure security, and control the propagation of personal information. Beyond these immediate benefits, this research presents an example that other developing countries may use to facilitate the adoption of biometrics technology.

Biometrics Technology: Understanding Dynamics Influencing Adoption for Control of Identification Deception Within Nigeria

by

Gideon U. Nwatu

M.B.A. University of District of Columbia, 1991

B.S. West Virginia University, 1983

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Applied Management and Decision Sciences

Walden University

May 2011

ProQuest LLC.
789 East Eisenhower Parkway
P.O. Box 1346
Ann Arbor, MI 48106 - 1346

Abstract

Biometrics Technology: Understanding Dynamics Influencing Adoption for Control of Identification Deception Within Nigeria

by

Gideon U. Nwatu

M.B.A. University of District of Columbia, 1991

B.S. West Virginia University, 1983

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Applied Management and Decision Sciences

Walden University

May 2011

Dedication

I dedicate this research to my dear and loving wife Ulo-o. Without her enduring love, great sacrifices, commitment, and support throughout this process, it would have been very difficult to overcome the many challenges and complete this scholarly journey. I truly and graciously express appreciation for her extraordinary dedication and understanding and for embarking on this journey with me. I owe my achievements to her. I also dedicate this work to our children, Obinna, Chibuzo, Ijeoma, and Chi-Chi for their support in several ways. I want to thank my parents, Mr. Paul Amadiegwu and Mrs. Bertha Nwatu, who sent me to the United States for further studies as a private student. They provided me a great opportunity that was necessary for accomplishing this professional and scholarly milestone.

Acknowledgments

I would like to give special recognition and extend my sincere gratitude to my mentor and committee chair, Dr. Raghu Korrapati, whose constant and consistent leadership and encouragement guided me through this journey and made this accomplishment a reality. I would not have completed this journey without his untiring support. I will always be grateful, Dr. Raghu. I would also like to thank my committee member, Dr. Stephanie Lyncheski, for contributing valuable insights and expertise that contributed significantly to the quality and validity of the final dissertation.

I extend my sincere thank you to Dr. Walter McCollum for his support in so many ways and also for introducing biometrics technology to me, which provided the genesis and catalyst for this study. I extend appreciation to each of the study participants who gave their time and attention and openly shared their attitudes, beliefs, and opinions. I thank Walden University's School of Management staff and faculty for their great support and encouragement through this journey.

I thank Elder Dr. John Oriji for all his assistance and encouragement. Finally, I extend my heartfelt thanks to Drs. Nnanna Okafor, Melesse Asfaw, Dominic Albert for unwavering collegial support; Jacob Mays of *SPSS tutor*, and Christine Weeber of *Stonefly Editorial Services* for professional services they provided to help me attain this academic accomplishment.

Table of Contents

List of Tables

List of Figures

Chapter 1: Introduction to the Study

Introduction

Biometrics technology has gained prominence since September 11, 2001, due to the terrorist attacks upon the United States (hereafter, 9/11; Hampe, Krulle, & Rebne, 2005). Few identification, authentication, and accountability mechanisms, such as password and personal identification number (PIN), surpassed the reliability of biometrics technology (AlBalawi, 2004; Harris & Yen, 2002). A biometrics security system has the capacity to confirm the presence of a person and potentially reduce the chances of identification fraud (Coventry, 2005).

The approach and need for high-confidence recognition and confirmation of individuals as citizens, employees, and visitors, as well as in consumer-related applications (International Biometric Group, 2007) highlights the growing imperative of biometrics technology for identification, recognition, and confirmation. The importance of utilizing biometrics technology can be seen in Figure 1. The model showed the relationship between biometrics technology, identification, access control, security, and tasks to be performed.

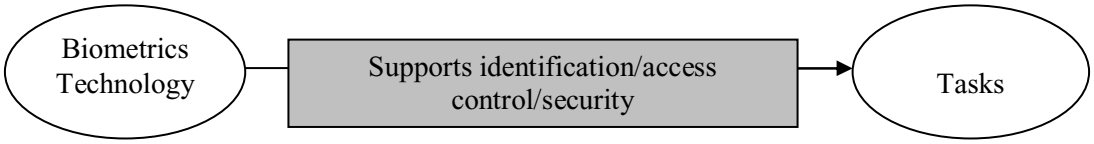


Figure 1. Biometrics technology supports identification, access control, and security.

In the paradigm shown in Figure 1, biometrics technology automatically and dependably verifies an individual's reference either through physiological (fingerprint) or

behavioral traits (signature; Acharya, 2006; Lease, 2005; Ngugi, 2005, Smith, 2005; U.S. Treasury, 2003). The system will bind the identified template to a user. This biometrics template provides mechanism for identification, authorization, and access control to sensitive areas, secured sites, or bank accounts, for tasks to be performed. The details of biometrics technology are presented in chapter 2.

In developed and developing countries, threats to national security, the desire to control crime, continuing immigration issues, and the need for access control to secure sites, locations, airports, and buildings provide justification for the adoption and application of biometrics technology (Anonymous, 2004; Brydie, 2008; Murphy, 2007; Tierney, 2001; Transportation Security Administration, 2008). Similarly, several studies and reports have highlighted the significance of biometrics technology application (Chandra & Calderon, 2005; Coventry, 2005; Gordon & Willox, 2003; Grijpink, 2005; Riley & Kleist, 2005) for the recognition, confirmation of identity, and crime control (Faulkerner, 2005; Global Security, 2009; Gordon & Willox, 2003; Kleist & Riley, 2005; Marburger, 2008; Opinion Research Corporation, 2002; Woodward, 2005).

Positive public attitudes and behaviors in developed countries regarding the use of the technology, despite privacy concerns, continue to increase (Brew, 2006; Brobeck & Folkman, 2005; Coventry, 2005; Giarimi & Magnusson, 2002; Faulkner, 2005; Matters, 2003; Sollie, 2005, Truste, 2005; Westin, 2002). This trend is expected to continue as terrorism and identity fraud posed increasing threats to the stability of national democracies and global commerce (Crowley, 2006; Gordon & Wilcox, 2003; Kristin & Erin, 2001; Willox & Regan, 2002). Despite this tendency, the concentration in

developed countries of studies, reports about adults' behaviors toward biometrics, and reasons for adoption creates an information gap.

This research bridged the disparity and contributed to a clearer understanding of the factors that influenced the adoption of biometrics technology for reliable recognition and confirmation in a developing country, such as, Nigeria. The sample of participants for this study comprised literate adults living within Surulere, Lagos, Nigeria. They were familiar with the technology. The study was mixed methodology research. An integrated methodology study approach was selected because data revealed adults' views linked to the adoption and usability of biometrics technology (Creswell, 2003). The survey and interview instruments were used to collect data. SPSS version 18, Microsoft Excel spreadsheet, Nvivo software version 7, content analyses, and frequency of percentages were used to analyze the collected data.

Although literature on biometrics abounds, scholars, consultants, scientists, and academicians most often use the term *biometrics* to describe the automated process or method of identifying and confirming the identity of human beings through individual distinctive physical characteristic or personal traits such as fingerprints and irises (Blackburn & Turner, 2002; Woodward, Jr., Horn, Gatune, &Thomas, 2003). "Biometric technology can not allow access to a system without unique identifiers. This is very important to restrict access and protect data (Jamieson, Stephens, & Kumar, 2005). Chirillo and Blaul (2003) stated, "Biometrics refers to authentication techniques that rely on measurable physiological and individual characteristics that can be automatically verified" (p. 1). The automated mechanism of recognition and confirmation of individuals made biometrics an important technique in the efforts to protect identity,

identify national security threats, control fraud, and enforce immigration policies (Gordon & Wilcox, 2003; Willox & Regan, 2002).

Biometrics technology has the potential to provide convincing evidence of who actually performed a given user transaction because each person's biometrics characteristics were thought to be unique and difficult to reproduce. In particular, biometrics traits were less susceptible to duplication or losses compared to other authentication methods and, as a result, provided a higher level of security (U.S. Treasury, 2003). For example, credit cards, passwords, and personal identification numbers (PINs) were conventional methods of authentication. However, biometrics characteristics such as the fingerprint and iris are integral parts of an individual (U.S. Treasury, 2003). These traits are difficult to forge or duplicate.

The growing weight of studies, surveys, and research showed the utilization of biometrics technology to address the issues of authentication and validation of identity (Acharya, 2006; Woodward, Webb, Newton, Bradley & Rubenson, 2001). Increasingly, many governments worldwide realized the importance of biometrics technology for identity management (IdM) (NSTC, 2006b; 2009c), crime, and access control (Campbell, 2005; SANS, 2002). Biometrics technology was the most definitive, real-time IdM tool that was more and more used for reliable verification (NSTC, 2009c).

The apprehension and the need for an increase in personal and national security also intensified the effort to implement biometrics technology for identity verification. Archarya (2006) reported about policies established that ensured funding, implementation, and administration of biometrics techniques in developed countries.

Both U.S. and Canadian federal governments have employed biometrics-based systems in several programs. Morgan and Krouse (2005) explained:

> The National Commission on Terrorist Attacks Upon the United States, commonly known as the 9/11 Commission, found that "constraining terrorist travel should become a vital part of counterterrorism strategy." Noting that "false identities are used by terrorists to avoid being detected on a watchlist" and that "biometric identifiers make such evasions far more difficult," the commission recommended that The Department of Homeland Security, properly supported by the Congress, should complete, as quickly as possible, a biometric entry-exit screening system, including a single system for speeding qualified travelers. (p. 1)

This recommendation and, in response to the 9/11 attack, the first phase of the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) program were implemented in 2004 (Acharya, 2006).

> The US-VISIT program, established by the Department of Homeland Security (DHS) and launched in 2004, collects, maintains, and shares information, including biometric identifiers, on selected foreign nationals entering and exiting the United States. US-VISIT uses digital finger scans and photographs to screen persons against lists (of criminals, terrorists and immigration violators), and to verify that a visitor is the person who was issued a visa or the travel document. (Acharya, 2006, pp. 10–11)

The imperative to identify and verify individuals led to the implementation of biometrics passports, which were required "of all travelers entering the United States, including U.S. citizens" (Morgan & Krouse, 2005, p. 2). In Canada, the Royal Canadian

Mounted Police (RCMP) upgraded its fingerprint identification system and improved its rapidity, exactness (Acharya, 2006), and effectiveness. Acharya further stated that the "new Automated Fingerprint Identification System (AFIS) will support the accurate processing of good-quality fingerprint submissions with little or no manual intervention" (Acharya 2006, p. 15). This AFIS minimized errors in identification and provided reliability in authentication.

In 2006, the British Parliament passed legislation that introduced biometric-related national identity (ID) cards. The government contended that this effort reduced identity fraud and illegal immigration and helped to decrease organized crime and terrorism (Acharya, 2006). Biometrics technology has been applied extensively and is indispensable to developed countries such as the United States, Sweden, and the United Kingdom, (Dror, 2006; Giarimi & Magnusson 2002 ; Jain & Ross, 2008; LogicaCMG, 2006; Sollie, 2005; Westin, 2002) but they were also becoming increasingly important to developing countries, for instance, Nigeria (Vanguard, 2006).

Recent reports indicated growing favorable opinions toward biometrics application in advanced countries (Giarimi & Magnusson, 2002; ORC, 2002). Research and reports showed increase in favorable public attitudes toward biometrics (Baird, 2002; Heckle, Patrick, & Ozok, 2007; Jain & Ross, 2008; Lawrence, 2005; Nakashima, 2007; Stephen, 2000; Towers Group, 2001; Westin, 2002). Therewas also increasing concern of privacy for the use of biometrics in developed countries (Crowley, 2006; Mordini & Petrini, 2007; NSTC, 2006a; Weber, 2006).

The privacy issues reported were function creep, mass surveillance, big brother, and informational (Acharya, 2006; Crowley, 2006; NSTC, 2006a; Weber, 2006). These

privacy apprehensions are discussed in chapter 2. As already indicated, some reports suggested application of biometrics security system in developing countries such as Nigeria (Vanguard, 2006). Nigeria is one of the emerging nations and biometrics technology has been implemented on a limited scale to provide a superior identification mechanism for the Nigerian National Pension Program (NNPP; Fingerprint Technology, 2006).

This effort was aimed to identify pension recipients and avoid individual mis-representation. Vanguard (2006) reported about the interest of using biometrics technology to curb identity fraud in the banking sectors. In Lagos, there was a seminar organized on "How best to identify consumers based on their physiological characteristics using their fingerprint or face to fight identity theft fraud in the Nigerian banking industry" (Vanguard, 2006, p.1). This showed the growing interest in biometrics in the banking industry in developing countries, such as Nigeria.

On the other hand, in developed economies, "Banks realize biometrics are not something to be ignored. Biometrics provides a unique advantage over other forms of security, such as user name and password, in that an individual's biometrics print is one-of-a-kind" (Bruno, 2001, p. 31). Consequently, the implementation of the technology was a positive development. While this was true in developed countries, however, the views of adults living in developing countries such as Nigeria should be explored relative to the factors that encouraged adoption. The data collected from the study helped to understand how perceived usefulness, ease of use, and security affected adoption. The failure to investigate and address these factors can impact wider acceptance.

In Figure 2, the research process is depicted, showing the components of the study.

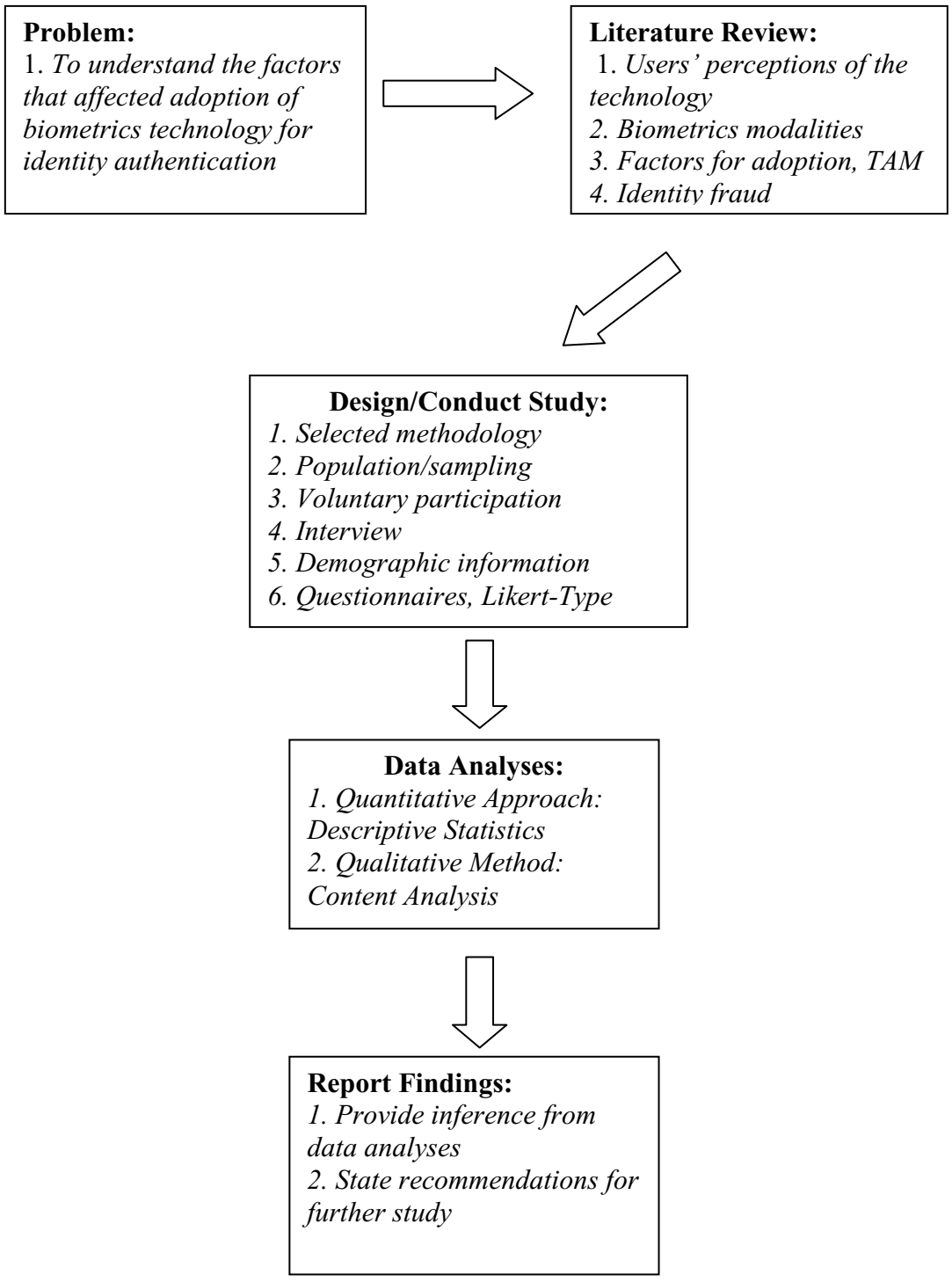


Figure 2. Graphic representation of the research process.

Statement of the Problem

The problem addressed in this study was the fact that identity fraud has been increasing in Nigeria due to lack of proper identification mechanism to credential people who commit identity deception. The problem addressed was linked to Joshua and Koshy (2009), who in a recent study concluded that perceived usefulness, perception of safety, and security influenced the attitude of users toward biometrics technology. In addition, Kim, Brewer, and Bernhard (2008) wrote that convenience, physical security, and data security were factors for implementation despite personal concerns of privacy. Similarly, Hsieh, Nguyen, and Lin (2008) cited ease of use and convenience when biometrics technology was used for payment mechanism to prevent identity theft. In another study (Seyal & Tajuddin, n.d.), researchers found that attitude was a significant factor that affected usability of biometrics technology. This study concentrated on the problem of identity fraud and the adoption of biometrics technology to mitigate control.

In developed countries, the perception, behaviors toward implementation and use of biometrics technology are positive (Anton, Earp & Jones, 2007; Brobeck & Folkman, 2005; Elliot, Massie & Sutton, 2007; LogicaCMG, 2006; Westin, 2002). Coventry (2005) suggested that "Users fundamental attitude toward a technology will affect their behavior with that technology" (p. 198). The study to leverage biometrics technology for mitigation of identity deception and verification of citizens was warranted (Chandra & Calderon, 2005; Fenn, 1999; Willox & Regan, 2002).

With the exception of Giesing (2003) in South Africa, to the best of the author's knowledge, no researchers have explored underlying factors that affect the adoption of biometrics technology for recognition, confirmation, and credentialing of individuals

within developing countries like Nigeria. Through the understanding of the issues, implementation strategies and policies could be prioritized for extensive application. The application of biometrics technology was important so that individuals were correctly identified, verified, because identity fraud and cyber crimes posed serious economic and financial consequences inside Nigeria. Moreover, identity deception was a harrowing experience for the victims (Smith, 2002).

The effort to control authentication deception has been ineffective because there was no reliable mechanism for recognizing and confirming people (Oghre, 2007). The implementation of biometrics security systems for instance, fingerprint was considered very important in maintaining and reliably confirming identity in the database (Acharya, 2006; Gordon & Willox, 2003). Consequently, this research was an empirical exploration that determined the influence of perceived ease of use, usefulness, and security, and awareness toward the adoption of biometrics security systems to control identity deception.

Background of the Problem

The proliferation of information communication technologies (ICTs) has been very dramatic, particularly in developed countries. According to Weber (2006), "Citizens of the developed world now live in an environment in which access to electronic information and communication is nearly ubiquitous" (p. 36) and the level of reliance on ICTs was unimaginable. For example, the Internet, which revolutionized communication and access to technology, has also increased global interaction and cooperation as well as commerce, entertainment, business, and scientific collaboration.

However, criminal opportunities have also been growing at an alarming rate due to the proliferation of ICTs (Weber, 2006). Identity fraud was one such criminal activity. An individual who pretended to be another person to acquire goods and services either through the creation of a fictitious name or from the acceptance of a real person's name (living or deceased) with or without authorization has committed identity fraud (Bick Financial Security Corporation, 2009; Dixon, Giskes, & Sampford, 2005; Smith, 2002;). Identity fraud has manifested as a global challenge and threat to the security of national governments, leaders, businesses, and citizens (Gordon & Willox, 2003).

Kim and LaCour (2009) stated that over 150 million U.S. consumers were concerned about IDF in online banking. The Javelin 2008 survey showed and confirmed that "nearly 10 million American victims losing $48 billion in 2008" and "The number of victims rose 22 percent to a record 9.9 million in 2008 from 8.1 million a year earlier, with about one in 23 U.S. adults becoming victim" (Stampel, 2009, p. 1).

In a global study conducted for Ipsos Public Affairs in 2008, researchers found that majority of online shoppers were concerned about identity theft and fraud (Jackson, 2008). In the United Kingdom, over 4 million Britons were estimated to be victims of identity fraud (Townsend, 2009). In a recent account, "The Australian Transaction Reports and Analysis Centre (AUSTRAC) found that identity fraud costs around $1.1 billion each year to Australia" (Dixon, Giskes & Sampford, 2005, p. 3).

Inside Canada, there were 7,778 confirmed cases of identity fraud reported in 2006 costing victims over $16 million in addition to emotional costs (Bick Financial Security Corporation, 2009). And in Nigeria, the escalation of identity fraud, cyber crime, and the advanced fee fraud "419" (financial crime) were growing (Oghre, 2007) and

generated international attention and negative publicity toward Nigeria and its citizens (Ayantokun, 2006; Gideon, 2002). It was, therefore, of significant interest to explore how ease of use, perceived usefulness, and security influenced the adoption of biometrics technology for control of identity fraud.

The events of 9/11 increased concerns about the contributory role of identity fraud in facilitating terrorism and other serious crimes (Stana, 2002). In light of the growing trend, however, there was no single data source that compiled and reported all incidences of identity fraud on a global scale. Understanding the threat of ID fraud was the foundation for response and ultimately helped to develop programs and policies to meet the growing challenges that it posed.

Researchers who studied identity fraud argued that it was an enormous global problem as well as a component of every major crime. According to (Gordon & Willox, 2003):

> Identity fraud, which encompasses identity theft, is the use of false identifiers, false or fraudulent documents, or a stolen identity in the commission of a crime. It often emanates from a breeder document created from fictitious or stolen identifiers. The breeder document, such as a driver's license or birth certificate, is used to spawn other documents, resulting in the creation of a credible identity which allows a criminal or terrorist access to credit cards, employment, bank accounts, secure facilities, computer systems, and the like. Once a criminal or terrorist has an established identity, he can use it to facilitate a variety of economic crimes, drug trafficking, terrorism, and other crimes. (p. 4)

Identity fraud was not only an issue in developed countries; it was of great concern to emerging nations like Nigeria. Identity fraud increasingly gained in notoriety in Nigeria (Oghre, 2007). Global Action (2008) reported that the level of poverty has worsened. It was not surprising that such level of social distress escalated the wave of identity fraud.

> Despite its plentiful resources of oil wealth, poverty is widespread in Nigeria. The situation has worsened since the late 1990s, to the extent that the country is now considered one of the 20 poorest countries in the world. Over 70% of the population is classified as poor, with 35% living in absolute poverty. (Global Action, 2008, p. 1)

Nigeria is rich in vast deposits of oil, natural gas, coal, and iron ore. Petroleum products are its main source of export income (Smith, Holmes, & Kaufmann, 1999). "Crude oil sales account for more than 90% of export earnings and around 75% of government revenue" (Smith, Holmes, & Kaufmann, 1999, p. 2) was derived from this source. Nigeria is a complex society—socially, economically, and politically (Oghre, 2007). The crime rate in the country was very disturbing. Oghre (2007) echoed this by stating that "the current state of crime in Nigeria means excesses and uncontrolled issuance of national documents by fraudsters and corrupt government officials, which requires us to have a system that will prevent double identities, multiple applications and abuse of the services" (p. 2). The author further argued that citizenship identification, recognition, and accountability were essential for law enforcement officials to effectively control crimes and ID fraud. This highlighted the importance of biometrics in providing identity-prone transactions.

In Lagos, organized fraud rings were common (Anonymous, 2007a). Lagos is heralded as "Nigeria's financial, commercial, and industrial nerve centre and has been categorized as one of the top 20 mega cities of the world with an active population of over 18 million people." (Lagos Economic Summit, 2008, p. 1) According to an Anonymous source (2009):

> Lagos is Nigeria's financial, commercial, and industrial nerve centre with over 2,000 manufacturing industries and over 200 financial institutions (banks, insurance companies and the like), including the nation's premier stock exchange, the Nigeria Stock Exchange. It also houses the nation's monetary authority, the Central Bank of Nigeria (CBN), and the Security and Exchange Commission (SEC). Indeed, the headquarters of multinational conglomerates like UAC, Unilever, John Holts, BEWAC/VYB, Leventis, Churchgate, Chevron, Shell, Exxon Mobil, and the nation's giant public enterprises are all located within the State.

This strategic location vis-à-vis other state capitals or cities made Lagos a prime candidate for this study. It attracted citizens, tourists, and international investors. The use of Internet cafes was increasingly popular. These cafes have often become breeding grounds for hatching ID and credit card frauds targeted at foreigners (Worldworx Travel, 2009). For instance, in September 2007, investigators from Nigeria, the United Kingdom, and the United States cracked down on fraudsters in Lagos who used postal services and transferred 15,000 counterfeit checks valued at $4 million (Anonymous, 2007a). "The anti-fraud police also found fraudulent identification papers and forged financial documents concealed in such a way as to prevent them from being picked up by security

scanners." (Anonymous, 2007a, p. 1) This underscored the growing rate of criminal activity involving fraud.

Nature of the Study

This mixed methodology descriptive study was designed to investigate the relationship between ease of use, usefulness, security, awareness, and behavioral intentions of adults living within Lagos, Nigeria toward the use of biometrics security system for identity recognition. This integrated approach was selected because it helped to better understand the research problem through the combination of numeric quantitative trends and the detailed of qualitative method (Creswell, 2003).

According to Creswell (2003), mixed methodology is:

> One in which the researcher tends to base knowledge claims on pragmatic grounds (e.g., consequence-oriented, problem centered, and pluralistic). It employs strategies of inquiry that involve collecting data either simultaneously or sequentially to best understand research problems. The data collection also involves gathering both numeric information (e.g., on instruments) as well as text information (e.g., on the interviews) so that the final database represents both quantitative and qualitative information. (p. 20)

Mixed methodology of qualitative and quantitative approaches was used to answer the research questions. This methodology was "part of a continuum of research with specific techniques selected based on the research objectives" (Sale, Lohfeld, & Brazil, 2002, p. 46). This researcher considered mixed method research necessary since "the complexity of human phenomena mandates more complex research designs to capture them" (Anaf & Sheppard, 2007, p. 186). Additionally, a mixed method design

"can not only enhance the data analysis opportunities for research (e.g., supporting qualitative themes with descriptive statistics), but it can further justify the sampling strategy of a project, and permit greater triangulation within research" (Anaf & Sheppard, 2007, p. 186). This was an important benefit of the integrated approach used for this study as was indicated in chapter 4.

The organization of the mixed methodological process involved major steps. In the first instance, the literature related to behaviors and intentions and attitudes toward application of biometrics technology for identification and verification was reviewed. Secondly, biometrics technology including the mainstream modalities and identity fraud were discussed. The factors that influenced adoption and the constructs of technology acceptance model were discussed. These are presented in chapter 2. A detailed discussion of the research methodology is presented in chapter 3. This study was descriptive and non-experimental.

The data from the sample population base has not been collected and measured for this type of study in previous national census development. Data for this research were collected through interview and survey instrumentations (Creswell, 1998; Tashakkori & Teddie, 1998; Viadero, 2005). The researcher recruited sample of study participants that resided within Surulere, Lagos. The answers from the research questions were measured and determined to what extent ease of use, usefulness, security, and awareness impacted the adoption and implementation of biometrics technique. Data were limited to the information that related to the research questions.

Research Questions

Purposive sampling was the proposed method used for data collection for the study. The data collected answered the following research questions:

1. What is the relationship between ease of use and adults' perceptions toward adoption of biometrics technology for control of identity fraud?

2. To what extent, if any, is biometrics technique considered a reliable mechanism for identity verification; and what is the relationship between perceived usefulness and the acceptance of biometrics technology for control of identity deception?

3. What is the relationship between security and adults' perceptions toward adoption of biometrics security for control of identity fraud?

4. What is the relationship between adults' awareness and the adoption of biometrics technology for control of identity deception?

Purpose of the Study

The purpose of the study of this mixed methodology study was to provide scholarly research about the factors that influenced the adoption and application of biometrics technology to reliably identify and verify an individual. A further reason of this study was to offer a platform to extend the literature beyond the commonly accepted theoretical frameworks to user technology acceptance and preference (Brydie, 2008) of particular biometrics traits in a developing country such as Nigeria. As already indicated, the integrated methodology was selected for this study so that it best conveyed the behaviors of individuals toward classes of biometrics technology such as fingerprint scan.

Since Nigeria has already implemented biometrics technology on a limited scale, this study was helpful and assessed the conduct of adults for a wider adoption of the technology. This provided more data from, which policy changes can be prioritized to implement the technique extensively. Understanding peoples' behaviors within Lagos was critical for broader adoption of biometric technology security systems to control ID fraud and be more proactive to maintain national and individual security.

The study was further expected to benefit the financial sector. Banks and their customers are victims of ID fraud. The implementation of identification and verification mechanisms will help banks reduce financial losses and protect customers' assets. Given the wave of financial crime in Nigeria, biometrics was an effective technique for preventing and controlling identity by reliably recognizing banks' customers. The maintenance of the names of convicts in the biometrics system's database was another advantage of adoption. Currently, Nigeria did not have a reliable system for credentialing, with almost all crimes committed going unpunished because the criminals cannot be reliably identified for prosecution (Oghre, 2007) and their names correctly managed in the biometrics database.

Theoretical Framework

The theoretical framework for this study was derived from the technology acceptance model (TAM), which Davis developed in 1989 (Klopping & Mckinney, 2004). It represented an important theoretical contribution toward understanding technology acceptance and usage (Malhorta & Galletta, 1999). TAM was derived from the theory of reasoned action (TRA) of Ajzen and Fishbein (Wahid, 2007), which

explained that virtually any human behavior consisted of two factors that affected behavioral intentions: attitudes toward behavior and subjective norms (Wahid, 2007).

TAM explained and predicted technology user behavior (Klopping & Mckinney, 2004). The Model was based on the idea that perceived usefulness (PU) and perceived ease of use (PEOU) influenced behavior and attitudes toward the adoption of new technology either negatively or positively. Rao (n.d.) suggested "that the attitude towards adoption depicts the prospective adopter's positive or negative orientation/behavior about adopting a new technology" (p. 2). Relevant internal beliefs helped and determined and influenced behaviors and attitudes. Several other factors, such as perceived ease of adoption, a user's apprehensiveness, the perceived utilities of the technology (Rao, n.d.) influenced users' attitudes and behavior toward adoption.

As already stated, the key components of TAM were perceived ease of use (PEOU) and perceived usefulness (PU). Wahid (2007) defined perceived ease of use as "the degree to which the prospective user expects the target system to be free of effort" (p. 3). If all things were considered, the easier it was to use a technology, the greater chance of a user's acceptability and adoption. The result and conclusion of this research supported this statement. Perceived usefulness was described as "a prospective user's subjective probability that using a specific application system will increase the user's job performance" (Wahid, 2007, p. 3). The result of analyses of qualitative and quantitative data also maintained this view in chapter 4. TAM further predicted that external variables such as characteristics of the system design, training, and available documentation may impact technology usage (Wahid, 2007).

The usefulness and ease of use affected the decision of adults to adopt biometrics technology. It therefore, implied that users believed biometrics technology helped them verified identity, effective in crime control; enhanced safety, and personal security. In this way, the effectiveness of the technology helped individuals to develop favorable mind sets toward application. This was therefore related to the theoretical framework of TAM.

Operational Definitions of Terms and Acronyms

There were several terminologies used in this study. In this section, the author defined specific terms, acronyms, and indicated their operational significance. The list of terminologies that were included provided readers the basis of definitions necessary for promotion of scholarly clarity and understanding (Brydie, 2008). This group of definitions was described in an informational approach that was consistent with how they were characteristically defined in the literature.

Access Control: This is a "technique used to permit or deny use of data or information system resources to specific users, programs, processes, or other systems based on previously granted authorization to those resources" (Bragg, Ousley & Strassberg, 2004, p. 789).

Accountability: The process of tracking and holding an identified and permitted user responsible for actions performed on the network (Bragg, Ousley & Strassberg, 2004).

Authentication is "the process of establishing confidence in the truth of some claim" and "the claim could be any declarative statement" National Science and Technology Council (NSTC, 2006a, p. 4) such as: the name of the person is John Doe.

"Authentication is sometimes used as a generic synonym for verification" National Science and Technology Council (NSTC, 2006a, p. 4).

Automated Fingerprint Identification System (AFIS): is "a highly specialized biometric system that compares a submitted fingerprint record (usually of multiple fingers) to a database of records to determine the identity of an individual" (NSTC, 2006a, p. 5). "AFIS is predominantly used for law enforcement, but it is also being used in civil applications" (Blackburn, Miles, & Wing, 2006, p. 5).

Attitude is a mental predisposition to act. It is expressed through the evaluation of an object either in favor or against. In the proposed study, attitude of users refers to the feelings and perceptions that are exhibited toward biometrics technology.

Acceptance is an agreement expressed through the conduct or act of using an object.

Adoption "is a process in which a technology is selected or rejected by an individual or Group" (Brydie, 2008, p. 10).

Biometrics is physiological or behavioral characteristics that are used to identify a person Weber (2006).

Biometrics technology is defined as an automated process of recognizing or verifying the identity of a living person based on a physiological or behavioral characteristic (Mordini & Petrini, 2007).

Biometric authentication is an automated process of establishing confidence in the truth of some claim of identity. It is an automated method of identifying or verifying the identity of a living person in real time based on physical characteristics or a personal trait. The phrase *living person in real time* is used to distinguish biometric authentication from

forensics, which does not involve the real-time identification of a living individual (Rand, 2001).

Big brother government refers to a state that controls or monitors the whole life of its citizens without consent (Rand, 2001; Weber, 2006).

Database is a structured collection of one or more computer files (NSTC, 2006a) organized for the contents to be easily accessed, managed, and updated. "These files could consist of biometric sensor readings, templates, match results, and related end-user information" (NSTC, 2006a, p. 10), which can be used in biometrics search.

Developed country is a country that typically operates with a modern infrastructure, an abundance of capital and skilled labor, a high development index and income, and an elevated standard of living compared to other emerging countries around the world.

Emerging country is a country that operates with an inefficient infrastructure, has an abundance of labor and a shortage of capital, usually preparing for development initiatives for economic development.

Ease of use refers to "the degree to which the prospective user expects the target system to be free of effort" (Wahid, 2007, p. 3).

Fingerprint is the unique pattern of ridges and valleys on the surface of a fingertip. This is formed during the final seven months of fetal development.

Fingerprint scan is the process of capturing the digital image or template of the fingerprint.

Global War on Terror (GWOT) is concerted effort and the necessary campaign to fight, defend against, and prevent acts of terrorism worldwide (Holetzky, 2009). Usually, this involves military, political, legal, economic, and ideological strategies.

Identity (IDf) fraud is the use of false identifiers, fraudulent documents, or a stolen identity in the commission of a crime. ID fraud has been used for decades by criminals and criminal organizations to help facilitate criminal activities and to avoid detection (Gordon & Willox, 2003; Kumar, Kuma, Lavassani & Movahedi, 2007; Smith, 2002).

Identity management (IdM) is "the combination of systems, rules, and procedures that defines an agreement between an individual and organization(s) regarding ownership, utilization, and safeguard of personal identity information" National Science Technology Council (NSTC, 2006b, p. 2).

Identification is "a task in which the biometric system searches a database for a reference matching a submitted biometric sample and, if found, returns a corresponding identity" (Blackburn, Miles & Wing, 2006, p. 17).

Information Communications Technologies (ICTs) are technologies used within the realm of communication and information systems.

Iris is the colored ring that surrounds the pupil and contains easily visible yet complex and distinct combinations of corona and other characteristics that can be analyzed and recorded as a mathematical template (Baird, 2002).

International Biometric Group (IBG) is the industry's leading consulting and technology service that provides technology-neutral, vendor-independent biometric services, strategies, and solutions (IBG, 2008).

Personal Identification Number (PIN) is a security method used to show what you know and, depending on the system, it can be used to either claim or verify a claimed identity (Blackburn, Miles & Wing, 2006).

Perceived usefulness is defined as "a prospective user's subjective probability that using a specific application system will increase the user's job performance" (Wahid, 2007, p. 3).

Security: The practice of protection and or safety without risk (Bragg, Ousley & Strassberg, 2004; Joshua & Koshy, 2009).

Task: A piece of job responsibility to be performed is a task (Answers Corporation, 2009).

Terrorism is broadly defined as politically motivated violence perpetrated against noncombatant targets by sub national groups or clandestine agents (Perl, 2003).

Technology Acceptance Model (TAM) is based on the idea that perceived usefulness and perceived ease of use will influence attitudes either negatively or positively in the effort to adopt new technology (Klopping & Mckinney, 2004).

Theory of Reasoned Action (TRA) is designed to explain virtually any human behavior and consists of two factors that affect behavioral intentions: attitudes toward behavior and subjective norms (Wahid, 2007).

U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT): is "A continuum of security measures that begin overseas, at the Department of State's visa issuing posts, and continue through arrival and departure from the United States of America" National Science and Technology Council, (NSTC, 2006a, p. 29).

Usability is the degree of ease and interest in using a particular tool, equipment, or technology.

Ubiquitous is the instance of being common, everywhere, or anywhere.

Verification is "a task where the biometric system attempts to confirm an individual's claimed identity by comparing a submitted sample to one or more previously enrolled templates" (Blackburn, Miles & Wing, 2006, p. 29).

Assumptions of the Study

The following assumptions were made concerning this research. The research subjects used in the study were good representation of the population of individuals living in Surulere, Lagos. The participants were literate (i.e., those who were able to read and comprehend the survey instruments presented to them). The survey participants were knowledgeable about biometrics technology but will not be users. The research subjects honestly answered the research questions to the best of their ability. The research subjects were aware of the increasing wave of identity fraud and the negative publicity it generated against Nigeria in international circles. The participants were assumed to know the function and importance of biometrics technology for identity authentication.

Scope and Limitations of the Study

It is acknowledged that there were limitations in the study. Surveys were common, usually easy to design, and familiar to respondents as "face-to-face interview, telephone interview, and questionnaire" (Leedy & Ormrod, 2001, p. 196). Surveys provided flexibility and standardization (Singleton & Straits, 2005). They were not adaptable compared to experiments and other methods because it was difficult to change

the course of research after the study had already started (Singleton & Straits, 2005). An important drawback of surveys was the introduction of systematic measurement error (Singleton & Straits, 2005).

The time and resources necessary to carry out full scope of attitudinal and behavioral intentions posed significant challenges. Since purposeful data sampling was used, the need to randomize was eliminated. That was a major limitation. Given that the exposure of the sample population to biometrics system was limited, compared to similar group in advanced countries, the outcome of the research was affected. The adults in developed countries were more familiar about biometrics technology through the media, literatures, vendors, and government sponsored programs. This was not the case in less developed countries such as Nigeria.

In consideration of the limited technical knowledge and experience of the participants, the majority of supporting data were obtained through surveys and interviews. The researcher relied on the openness and trustworthiness of the participants and this affected the validity and reliability of the study since the researcher had no control over the participants. The study was carried out in Nigeria and the participants were within the geographical location of Lagos State. The conditions in a neighboring state were not identical. This limited the researcher's ability to make generalizations of the study's result in other surrounding states.

A number of researchers expressed concern about age and gender playing detrimental role affecting the external validity of opinion based studies (Brydie, 2008). This presented an important limitation. Since the participation in this study was

exactingly voluntary, it was impossible to determine the age variation and gender segmentation of the population (Brydie, 2008).

Delimitations of the Study

The delimitation of this research was that the adult participants comprised people living in Surulere, Lagos. They were from banks, government offices, and public places. The results of the study would have been different if it was conducted in another city or state in Nigeria. The study was limited to research subjects who did not have difficulty completing the survey and interview instruments. This study was conducted overseas; Lagos, Nigeria. Therefore, financial resources constrained the author's efforts. The investigator also navigated logistical impediments such as seasonal weather, bad roads, antiquated ICTs, and frequent power outages. Finally, other variables such as small sample size due to purposeful sampling provided quicker results. However, it served as a delimitation factor.

The Significance of the Study

This study provided considerable importance in the following areas: management field and profession, information systems management (ISM), body of knowledge, and as a resource to control identity fraud.

Management Profession

There is growing concern about the vulnerability of something an individual knows (password) and has (token). These items have been used for identification and authentication of people both inside corporation, organization, and airport facilities. As people live in the era of digital kingdoms, computer slaves (Sukhai, 2004), and the

ubiquitous information communication technologies (ICTs), the need to reliably and correctly verify employees and individuals was challenging. This study highlighted that biometrics technology if adopted was a technique that can be used to confirm the identity of employees both for access control to secured environments and the privilege of conducting tasks that have national and corporate magnitude. In most situations:

> People require varying degrees of access to certain buildings, facilities and/or resources. Intruders may try to gain access for the purposes of espionage or sabotage. Photo or other passes/smart cards can be used to manage access by authorized persons and to keep out intruders, but the possession of a pass or smart card alone does not guarantee that the holder is the person authorized to use the pass. (Heyer, 2008, p. 33)

Therefore, a biometrics security system has the capacity to confirm the presence of a person and potentially reduced the chances of identification fraud (Coventry, 2005). Through the process, only identified, authenticated, and authorized employees would have access to secured data if biometrics security system was implemented. This did not eliminate the work of insiders for suspicious activities, Sukhai (2004). However, management was in a better position to know those that have access, identify them, and investigate the individuals. Understanding the factors that influenced adoption of biometrics technology helped management for employee identity management.

There are several biometrics techniques and each was very effective in different circumstance; such as the iris, which has lowest error rate (Lease, 2005), and was suitable for implementation at the airports. Fingerprint, considered as the biometric modality that has the longest history and has been most extensively deployed (Lease, 2005;

Rosenzweig, Kochems, & Schwartz, 2004; U. S. Treasury, 2005), was best suited for identification and verification. Managers of information technology and network infrastructures would be aware that the adoption of biometrics technology to identify employees, control physical and logical access, and secure resources and assets was a rational choice.

The result of this study further proved to management the information that biometrics once adopted was relevant in managing personnel—particularly for the administration "of personnel identities, safety systems, payroll and leave" (Heyer, 2008, p. 34). The author further stated that "the US transportation sector recently introduced the Transport Workers Identity Credential or TWIC, which uses fingerprint and face for access control and identity management" (Heyer, 2008, p. 34). Such mechanism provided identification assurance to management.

Information Systems Management (ISM)

In managing information systems, this study highlighted how leveraging biometrics technology provided reliable mechanism for identification, authorization, and access control to information assets and resources. One of the significances of this integrated methodology study was its contribution to information systems management (ISM) literature. Sukhai, (2004) stated that "Proper identification, authentication, authorization, accountability are the components of access control" (p. 125). The security and protection of information systems depended on the employee's right of entry to secured sites of protected data. Biometrics technology was a crucial component of secure personal identification and verification schemes, which controlled access to valuable information systems. The result of this study provided data that showed factors that

influenced adoption of biometrics technology in order to realize the benefits of the system.

Biometrics-based identification and verification systems supported the information infrastructures both on national and global scales (Radack, 2009). This was important for the confidentiality, integrity, and availability of corporate data (Sukhai, 2004). The main server areas and communication links of information systems were vulnerable to risk. Additionally, unauthorized users may access corporate data on the network through unsecured software. These two types of vulnerabilities reduced using biometrics security mechanism (Heyer, 2008). For instance, fingerprint sensors on the keyboard and iris recognition can be used for logon right of entry. This will ensure that users are granted only the appropriate level of access. In turn, corporate data, information assets, and resources are secured from breaches and compromise through the implementation of biometrics technology.

Body of Knowledge

Several studies that included Jones, Anton, and Earp (2007), Elliot, Massie, and Sutton (2007) examined attitudes and behaviors toward adoption of biometrics security system in developed countries. These researchers, however, did not explore the potential of other dynamics that influenced implementation of biometrics technique for identity verification not only in the developed nations but in the developing countries such as Nigeria. This created a knowledge gap. The study helped to close this gap by revealing certain factors that affected the adoption of biometrics security system in a developing country.

This study further exploited the opportunity and added to the existing body of knowledge about the relationship between the dynamics for adoption of biometrics security technique and the need to control identity deception. While the opinion of biometrics technology users and non users in developed countries has attracted considerable research, no studies focused on emerging nations. As a result, practitioners do not have empirical data model on developing countries for instance, Nigeria. This study provided statistics and highlighted the views of adults toward greater acceptance of biometrics technology for identity management and control of crime. This study was among the first that addressed the factors that were necessary to influence the adoption of biometrics technology within Nigeria for control of identity fraud. Majority of previous studies concentrated in developed countries albeit, not in developing nations. Practitioners have empirical data model on a developing country. This provided opportunity for further and future inquiry.

Technique to Control Identity Fraud

The dangers and consequences of identity fraud and the threats of terrorism are real and are increasing on a global scale. It was therefore critical to address these issues. Biometrics technology, which has been "viewed as providing better security, increased efficiency, and more reliable identity assurance than other commonly used methods of authentication/identification based on what a user possesses or what a user knows" (Lease, 2005, p. 19), provided potential benefits in identity verification and administration.

The study provided the Nigerian government actionable strategies for controlling crime. The result of this study offered government guidance to overcome obstacles (NSTC, 2006b) that prevented a wider implementation of biometrics technology. Specifically, the government would assist in the promotion of guidelines necessary to achieve public and private collaboration in identity management technologies.

The result provided informative examples of integrating biometrics systems into society (NSTC, 2006b) for recognition and confirmation of individuals. It stressed the importance of awareness and the advantages of using biometrics for safety and personal security. Another benefit of this study was for Nigerian government to share data with friendly countries in an effort to arrest and prosecute individuals involved in drug trafficking, financial crimes, money laundering, and immigration concerns.

The study also gave lawmakers a basis to enact legislation that would encourage the application of biometrics technology. Such efforts would help ease apprehensions and assured the citizens that measures to control crimes are being undertaken. In addition, the study provided vendors the data upon which implementation and marketing strategies of biometrics technology would be developed to overcome any negative behaviors and to bring about user acceptance. The technology developers would "undertake present and future challenges in determining which class of biometric technology provides the most adequate levels of privacy and security without being perceived as invasive by clients and potentially affecting overall profitability" (Brydie, 2008, p. 10). This would translate to increased return on investment (ROI) for such project.

The negative publicity from crime has discouraged foreign investment and impacted tourism, social, and economic industries in Nigeria. The result would help

promote efforts to control crime and, therefore, ideally, minimize adverse publicity and encourage industrial and economic investments from foreign investors and multinational corporations.

This study has implications for positive social change. Crime is an impediment to economic and social stability. For a government to bring about positive social change, the unrest in the society resulting from law-breaking and its consequences must be addressed. There was little argument that the economic and political strength of a country affects its social stability. The control of offenses provided favorable environment for economic growth and social stability. As the global war on terror (GWOT), identity fraud, money laundering, and other criminal activities continue to intensify; nations such as Nigeria would have the social responsibility to control them due to domestic and global consequences.

Biometrics technology serves as an appropriate tool for the authentication and maintenance of individual identities. The technology would also ensure that criminals were correctly identified and legitimate persons maintained authorized access to secured sites, bank accounts, and other privileged data. This investigative study further helped and measured the extent to which individuals believed the usefulness of fingerprint for controlling crime even if they do not have interest to utilize the security system.

Summary

Although critics continued to debate the issue of biometrics as an invasion of privacy, the urgent necessity of identifying, verifying, and protecting citizens was acknowledged both nationally and globally. The consequences of not correctly

recognizing and confirming individual identity were dire. The tragedy of 9/11 has not been forgotten, in addition to the growing trend of ID fraud that posed significant threats to individual security and societies. Biometrics technology was widely accepted as the preferred method for fighting ID fraud. Researchers in developed countries have documented the public's favorable views toward biometrics technology as well as user acceptance despite privacy concern. This study contributed to such understanding and identified the dynamics that influenced adults' behavior toward adoption.

Nigeria has implemented biometrics (fingerprint) technology for classified pension recipients. However, the factors that will enable wider implementation and administration of biometrics techniques have not been explored. Ease of use, usefulness, and the need for individual security, and awareness affected adults' attitudes and perception, which in turn greatly influenced the adoption and acceptance. Given the seriousness of identity fraud, it was important that decision makers have an understanding of these issues.

The growing importance of biometrics technology for recognizing and confirming identity was discussed in this chapter. This researcher also provided an overview of the problem of ID fraud and the potential solution found in biometrics technology, discussed the nature of the study, and outlined the significances of the study. Additionally, this author also examined the scope of the research as well as the questions that guided this study.

In chapter 2, a review of the literature from doctoral dissertations; journal articles, online databases, technical publications, white papers, and studies on attitudes, behaviors toward biometrics technology is presented. The underlying reasons that affected usability,

the technology acceptance model (TAM), history, overview of biometrics technology, and mainstream modalities were discussed. Furthermore, fingerprint technology as the mature and popular biometrics trait for identification and verification, despite its common-criminal stigma association was presented.

The researcher ends chapter 2 with a discussion of identity fraud, its consequences, and as a major rationale for the growing interest for the implementation of biometrics security system. In chapter 3, the research design, approach, and detailed description are presented. The investigator discussed selected research approach and the justification, the study design, sample selection, data collection, and analytical methods.

Chapter 2: Literature Review

Introduction and Organization

The objective of this chapter was to review the literature and gain a better understanding of factors affecting the adoption of biometrics technology, which is heralded as a significant tool for preventing identification and authentication deception. The chapter also examines identity fraud and its consequences and the growing interest in using biometrics technology as a control measure. At present, this study is valuable because the attention to factors that affect the adoption and acceptance of biometrics technology both in developed economies (LogicaCMG, 2006; Westin, 2002) and in developing countries such as Nigeria (Oghre, 2007; Vanguard, 2006) has been increasing. The implementation of a biometrics system is important for identification, verification, and for controlling identity fraud (Gordon & Willox, 2003; Norman & Thomas, 2005; Unisys, 2005).

Brydie (2008) posited that trust and reliability impact the usability and application of biometrics. In contrast, Kim (2006) stated that convenience affected user acceptance of biometrics. Other authors have argued that perceived ease of use, perceived usefulness, influenced adoption and affected acceptance (Jahangir & Begum, 2008, Joshua & Koshy, 2009; Klopping & McKinney, 2004; Wahid, 2007). Sasse (n.d.) further argued that concerns for security, trust, and convenience led to user acceptance and adoption.

This chapter is organized into six different sections. In the first section, the researcher analyzed relevant studies about attitudes and behaviors that affected the adoption of biometrics system, as well as the problems identified with the technology. The second section illustrated the need for and the usability and acceptance of biometrics

technology. The third section discusses the history of biometrics technology and mainstream modalities as well as errors of the system. Fingerprints as an industry de facto technique that has universal application despite the common-criminal stigma associated with it is also presented.

In the fourth section, this researcher outlines the criticisms and privacy concerns surrounding biometrics technology. The technology acceptance model (TAM) as the theoretical framework pertinent to this study was presented in section five. This model postulated that the behavioral intention to use and apply new technology will depend on the perceived usefulness (PU) and perceived ease of use (PEOU) (Klopping & Mckinney, 2004; Ngugi, 2005; Wahid, 2007). When users believed that biometrics technology provided security and reliably identified individuals involved in fraud and other criminal activities, they would have favorable opinions toward the adoption and use of the technology.

In part six, identity fraud (IDF), including the growing global trend, is discussed (Gordon & Willox, 2003, 2006; Regan & Willox, 2002; Unisys, 2005). The section presents an overview of the crimes committed through IDF. It is important to highlight IDF because the losses and consequences of identity theft are growing every year (Choo, Gordon, Gordon, & Rebovich, 2007; Kim, 2006; Unisys, 2005). Biometrics security technique is expected to play an important role as a control measure. In the final section, the researcher summarized the chapter.

The Literature Review

According to Sollie (2005), the literature review is based upon an effort to search for and obtain information relative to a study for the purpose of offering a critical appraisal. The texts on biometrics technology, attitudes, identity fraud, and other pertinent scholarly literature were obtained from ProQuest databases through Walden University; the library of Strayer University Alexandria, Virginia; the Accokeek Library of Prince Georges County, Maryland; the Digital Repository at the University of Maryland; and recent professional journals, business publications, technical reports, white papers, newspaper articles, magazines, EBSCO Hosts, and online databases. The method used and searched appropriate texts included the use of key words, phrases, and titles. In addition, other data were obtained from the review of several doctoral dissertations on the concepts, subjects, and researches relevant to the topic of this study.

Part 1: Attitudes and Behaviors Toward Biometrics Technology

Attitudes toward biometrics are rapidly increasing because the technology is becoming widely accepted as people recognized its security benefits (Sherwood, 2008). The system's ability to provide identification and verification for credentialing individuals are major benefits. A person's attitude toward technology is a major determinant for the adoption, acceptability, and usability of that technology. For example, an individual with a positive impression and attitude toward biometrics technology will exhibit positive behavior toward using biometrics technology.

Conversely, negative attitudes means an individual will hesitate to accept biometrics system. The studies that examined the attitudes of users of technology have

been drawn extensively from theories of innovation adoption and social psychology (Lease, 2005). Theories such as the technology acceptance model (TAM) of Fred Davis (Alrafi, 2005; Malhorta & Galleta, 1999), the theory of reasoned action (TRA) of Ajzen and Fishbein (Wang & Liu, n.d.), and Roger's diffusion of innovation theory (Chaffey, Chadwick, Mayer, & Johnston, 2006) helped to describe the attitudes and behaviors of individuals toward adoption, perception, and acceptance of technological systems.

These theories explained the paradigms of approval and usability of technology. Attitude is an essential barometer of human psychology that controlled behavior. The attitude–behavior relationship influenced adult's positive or negative affirmation toward technology acceptance. An affirmative attitude encouraged the use of biometrics technology. On the other hand, a pessimistic mindset will discourage the use of biometrics systems. Once attitudes are formed according to the attributes of relevant technologies, such beliefs either will enhance or diminish acceptability, usability, or influenced adoption (Coventry, 2005; Lease, 2005).

Emerging bodies of studies showed the importance of biometrics technology (Brobeck & Folkman, 2005; Giarimi & Magnusson, 2002; Ngugi, 2005; TRUSTe, 2005) and the increasing concern for privacy (Crowley, 2006; Electronic Frontier Foundation, 2006; Mordini & Petrini, 2007; National Science Technology Council [NSTC], 2006d; Weber, 2006). In developed countries, the increase in positive user attitudes toward biometrics was not surprising, given the attacks on September 11, 2001. Several relevant studies explored adult mindsets toward recognition technology (Brobeck & Folkman, 2005; Faulkner, 2005; Jones, Anton, & Earp, 2007; Westin, 2002).

Though these studies on the factors affecting acceptance, attitudes, and behaviors of users toward biometrics are generally carried out in developed countries, the researcher was surprised to find that except the study of (Giesing, 2003) on user perception in South Africa, no other investigation explored issues related to biometrics technology adoption in emerging countries such as Nigeria. Nigeria is an advancing country, albeit not on par with any of the developed nations; however, it is developing rapidly. That notwithstanding, this author argues that it is necessary that a study be conducted to determine the relationship between causes of implementation and adult attitudes toward biometrics technology acceptance within Lagos, in Nigeria. The results of this research will help to determine appropriate biometrics techniques and strategies for wider application in an effort to control identity fraud. The role that biometrics played in verification and confirmation to prevent identity deception has prompted several studies to determine issues that affected adoption and acceptance.

In an examination that focused on user behaviors toward authentication technologies, Jones, Anton, and Earp (2007) argued that “Biometrics appear to be the most popular method of authentication in general, with half of all respondents agreeing that they would prefer to use biometrics to verify their identity as opposed to tokens or passwords.” (p. 93) Passwords can be shared but biometrics was unique to a particular individual and cannot be given to someone else.

The study, which involved 138 respondents between the ages of 18 and 21, revealed that 51% of users were familiar with biometrics modalities such as fingerprint scan, 47% were familiar with signature analysis and 44% with voice recognition while user password awareness was 94% (Jones, Anton, & Earp, 2007). This is not surprising

since password is common with users of information technology. From the statistical data, the authors concluded that the usefulness of biometrics technologies were far better than passwords and tokens.

Jones, Anton, and Earp (2007) also cited biometrics usefulness in the areas of building access to be 47%, access to doctor's office or hospital at 54%, financial transactions at 66%, and online transactions to be 44%. The usefulness of technology was one of the constructs of Technology Acceptance Model (TAM) (Ngugi, 2005), which is discussed in section 5 of this chapter. If users were aware of the benefits of biometrics, that will affect acceptance and usability. However, the authors found that 77% of respondents preferred the use of passwords in computer access and 66% preferred it in financial transactions. Though the use of passwords for computer access has been preferred, there is a growing concern about the vulnerabilities of passwords for identification and the right to use network resources (Smith, 2005).

King, Lee, Turban, & Viehland (2004) stated that "passwords are notoriously insecure because people have a habit of writing them down in easy-to-find places, of choosing values that are easily guessed, and of willingly telling people their passwords when asked." (p. 474) A better approach is a two-factor authentication that combines a biometrics modality, such as fingerprint, and a password or multi-biometrics authentication (King, Lee, Turban, & Viehland, 2004; Jain & Ross, 2004). This will provide protection and prevent circumvention of security policy.

In another study that involved 391 respondents, there was overwhelming support for biometrics applications in law enforcement and in obtaining passports (Elliot, Massie, & Sutton, 2007). This study confirmed favorable perceptions of biometrics and

substantiated previous research by Unisys (2005) and Westin (2002). Similar to the findings of Elliot and colleagues, LogicaCMG (2006) conducted a study and stated "that consumer attitudes have reached a tipping point where most consumers are now convinced that biometrics such as iris scanning and fingerprints are both safe and accurate" (p. 1). This study involved 500 participants in seven different European countries.

In 2001 and 2002, Westin (2002) conducted a study in the United States. The purpose of the investigation was to measure the public's attitude toward the use of biometrics for identifying persons more accurately and for helping in the prevention of crimes such as identity fraud. The findings showed stable awareness of biometrics technology after the events of September 11, 2001, among affluent and college-educated respondents. Among the respondents who provided identifiers, fingerprint scanning was the most familiar technique that 70% experienced in 2001 and 82% in 2002, followed by signature dynamics (34% in 2001 and 46% in 2002; Westin, 2002, p. 4).

The survey further showed that 88% of respondents accepted law enforcement authorities when they required fingerprint scans to verify identity, 84% accepted fingerprint scans to obtain entry into government buildings while 82% were accepted at airport check-ins and 77% accepted when obtaining a driver's license (Westin, 2002). In 2005, TRUSTe (2005) conducted a similar study and noted favorable attitudes toward biometrics technology. The participants in the study responded according to the following: fingerprint 81%, eye (iris) scan 58%, hand geometry 50%, and voice recognition 48%. Conversely, the outcome of the research showed a non-acceptance rate of 8% for fingerprint, 17% for iris scan, 16% for hand geometry, and 20% for voice

recognition (TRUSTe, 2005). The study clearly showed the growing awareness of biometrics system in identity management.

Perhaps the events of September 11, 2001 reduced public objections to privacy concerns and contributed to the consciousness of biometrics technique among national and international governmental entities, individuals, and businesses (Brobeck & Folkman, 2005; Faulkner, 2005; Lease 2005; Unisys, 2005). In a study by Faulkner (2005), participants agreed that biometrics offered protection against identity theft. It was likely that press publicity and television news generated awareness and concern for this issue among the masses (Faulkner, 2005). In Sweden, Brobeck, and Folkman (2005) carried out a study about the attitudes and factors that influenced a breakthrough in biometrics. Though the authors argued that costs hindered companies from implementing biometrics, they did conclude that fingerprint was a popular biometrics technique that is matured, trusted, and preferred (Brobeck & Folkman, 2005).

The change in security requirements for accessing resources on the network was another reason for positive attitudes toward biometrics technology. Passwords have been used for log on recognition and verification for secured access. However, users are growing weary of using different passwords for various accounts. The user community is frustrated by the need to create and remember dissimilar and complex passwords. Biometrics technology is seen as an alternative to periodically changing complex passwords.

In addition, in a survey that Unisys (2006) conducted, 82% of respondents cited convenience as the top benefit of biometrics technology. The participants in the study demonstrated a growing interest in biometrics because it offered convenience and

protection. Kim (2006) argued and concluded that convenience, physical security, data security, and personal privacy affected acceptance of biometrics. The author conducted the study in Las Vegas and found that hotel customers were open to the technology as alternative identification and validation approach.

Although the significance of biometrics is growing, several problems with the technology have been identified. One was the effectiveness of the biometric reading sensor (BRS) (Vance, 2002). The accumulation of dust, lotion, and hand cream can render the system's sensor inefficient and unreliable (Vance, 2002). This can lead to errors such as when access is granted to the wrong individual or the person is not correctly identified.

A second problem is that most biometrics systems are optically based and may perform poorly when there was not sufficient lighting, such as with face and iris recognition systems (Savastano & Riccardi, 2005), which are appropriate for indoor use. The lighting condition can significantly reduce the available options for biometrics system. This is important since every biometrics technology may not be suitable for all situations (Liu & Silverman, 2001). The user acceptability is of primary importance to guarantee success of adoption and implementation (Savastano & Riccardi, 2005). For instance, fingerprint technology usually has criminal stigma and people were always concerned when it is mentioned.

Fingerprints have a tendency to change over the interval of a six-week period due to degradation (Harrison, 2002) and, in most cases; aging affects some biometrics traits, such as fingerprints and the human face. Lanitis (2009) wrote that the effect of aging on facial recognition leads to "inconsistencies between facial features stored in the template

and the features derived from a face of the corresponding subject" (p. 142). This can trigger errors when identification is initiated. Further problems are accuracy, scaling, security, and privacy (Hing, Jain, Pankanti, Prabhakar, Ross, & Wayman, 2004).

The promise of the ideal biometrics technology to provide a correct decision when a sample is presented to the system has not been achieved, which resulted in two critical errors: false match and false non-match (Hing, Jain, Pankanti, Prabhakar, Ross, & Wayman, 2004). These errors will affect the proportion of acceptance and rejection. They affected the performance of the system and more of them are presented in section three of this chapter.

An additional problem with the technology is the size of the database, which will affect real-time applications. It is important to scale the system according to the size of applications involving large amount of data transactions and for efficient throughput. When this is not achieved, in most cases, it becomes a major concern for storage and execution. Another concern is no secrecy about biometrics when it is breached and it is not irrevocable (Hing, Jain, Pankanti, Prabhakar, Ross, & Wayman, 2004). For instance, when passwords are stolen or lost, they are changeable for confirmation and access privileges. However, when a biometrics template is compromised, it cannot be replaced.

Therefore, it is very difficult to correctly and reliably verify the individual that had the reference that is compromised. The template stored in the database will not be the same as the data derived from the person during a live capture. This might lead to an error of false acceptance. Similar to this problem is the breach of the central database where the templates are stored. If hostile attacks are launched on a trusted and secured central database where biometrics templates are saved, users' biometrics will be

compromised for life. Another significant concern is the person responsible in the event that biometrics data are stolen. This is an issue that (Shafir, 2006) contemplated. These are some of the major problems of the technology. In part four, further criticisms of biometrics are discussed.

Part 2: The Need and Use of Biometrics

There is an increasing interest in biometrics technology for crime control and identity credential (Blackburn, Coty, Cook, Dee, & Dunn, 2008; Radack, 2009). The need to reliably confirm and verify people and to control identity fraud and monitor online banking and e-commerce, and the growing threat of global terrorism make it an imperative to implement biometrics technology to support identity management (AuthenTec, 2008; Radack, 2009).

The European Commission supported this argument and stated that the ability of biometrics "to increase trust in identity authentication is their greatest advantage" (European Commission, 2005, p. 73). Lease (2005) also wrote that "ensuring the identity and authenticity of persons is a prerequisite to security and efficiency in modern business operations. Unauthorized intruders can damage physical and logical infrastructure, steal proprietary information, compromise competitiveness, and threaten business sustainability" (p. 14). The ability to recognize individuals is very crucial in the context of the global war on terror (GWOT) and the growing threat of identity deception (Gordon & Wilcox, 2003; Unisys, 2005, 2006).

Biometrics systems are critical "in the larger national and homeland security context both in the US and internationally" (Markowitz & Gravell, 2007, p. 7). It is, therefore, not surprising that national and world "governments will continue to apply

biometrics in their efforts to make society safer,…it is the public that will stimulate the growth of the market in biometrics through their desire to live a life made easier by new technological innovation" (Reedman, 2004, p. 5).

In a report "FBI Prepares Vast Database of Biometrics: $1 Billion Project to Include Images of Irises and Faces," Nakashima (2007) wrote, "The FBI is embarking on a $1 billion effort to build the world's largest computer database of people's physical characteristics, a project that would give the government unprecedented abilities to identify individuals in the United States and abroad" (p. A1). Other factors such as these combined and supported the need for biometrics technology:

1. Awareness and global intensification of anti-terrorism post 9/11.
2. Acceleration of identity, Internet, and other forms of frauds.
3. Increase in public recognition of the benefits.
4. Reduction in errors and improvement in accuracy.
5. Need to control the boarder thorough identity recognition.

The experience of 9/11 further intensified the need for security of individuals and visitors. Research conducted in European countries (LogicaCMG, 2006), the United States (Westin, 2002), and global surveys (Unisys, 2005, 2006) showed the growing importance of biometrics systems despite concerns about privacy.

Giesing (2003) conducted a study in South Africa and noted the opinions of research respondents toward biometrics in the following manner:

1. Biometrics as a possible means of identification will satisfy their security concerns.

2. Biometrics will ensure that only authorized users gain access to certain information.
3. Biometrics is a good idea because a user's identity cannot be reproduced by someone else—uniqueness.
4. Biometrics is a more workable solution than traditional identification methods because it is easier to use.
5. The use of biometrics as a possible means of identification will provide more confidence in the security of on-line transaction. (p. 124)

The American National Standards Institute [ANSI] (2007) argued that the need for and use of a biometrics system depended on its performance. Sasse (n.d.) also stated that user acceptance of biometrics was the function of three criteria: "performance, user satisfaction, and user cost" (p. 1). These criteria are important for biometrics developers and vendors to consider when designing and manufacturing biometrics system. The performance of the system and each user's ability to complete tasks are equally important. The perceived usefulness of the technology and each user's satisfaction largely will depend on the assessment of speed and ease of the interaction (Sasse, n.d.). The effect of this interface will affect adoption.

This author believes that the cost to users and the thought that goes into using the system should be considered. The costs are the physical and mental efforts required to interact with the system (Sasse, n.d.). Sasse further stated that three important factors that will lead to user need and adoption were: a concern for increased security, convenience, and trust. Two other researchers came to the same conclusion (Brydie, 2008; Kim, 2006). However, American National Standards Institute [ANSI] (2007) wrote that the expected

tangible benefits of biometrics systems to users determined the extent of acceptance. Sasse (n.d) noted that a willingness to use the system diminished substantially if the user did not perceive potential benefits. In section three, the overview of biometrics technology, mainstream modalities, system errors, and fingerprints as industry de facto technology are discussed.

Part 3: Biometrics Technology

History and definition. The history of biometrics is very fascinating, following many centuries of development, improvement, and implementation. Biometrics technology increasingly drew interest as protection, identity fraud, access to secured applications, and privacy were more important to the security industry, various governments, the corporate world, and in public and individual circles (Chirillo & Blaul, 2003; Jamieson, Stephens, & Kumar, 2005; Lease, 2005; Rosenzweig, Kochems, & Schwartz, 2004; Short, 2002).

Early in civilization, human-to-human recognition occurred through the human face, which has been one of the oldest and most basic examples of identification. Biometrics has been used for recognition since at least the time of the Pharaohs, who used height measurement and verified a person's identity (Baird, 2002; Davis, 1994). In the mid-1800s, the rapid growth of cities and the increase in human population due to the industrial Revolution as well as more productive farming made the need to identify people very important (Anonymous, 2006). During the late 1800s, there was a robust method called the Henry System for indexing fingerprints. True biometrics systems, however, did not begin to emerge until the latter half of the twentieth century, coinciding with the emergence of computer technology.

There are various definitions of biometrics in the literature. The term biometrics is derived from the Greek word *bio* (life) and *metrics* (to measure) (Anonymous, 2007d; Zorkadis & Donos, 2004). According to Jamieson, Stephens, and Kumar (2005), a *biometrics system* is an "automated method of verifying or recognizing a living person on the basis of some physiological characteristics, such as fingerprint or iris patterns, or some aspects of behavior, such as handwriting or keystroke patterns" (p. 1). Similarly, biometrics is the science of measuring physical properties of living beings (Bromba, 2007). In addition, other authors such as Baird described the terminology.

Baird (2002) defined it as "the science of using digital technology to identify individuals based on the individual's unique physical and biological qualities" (p. 1). In principle, biometrics technology used one or several physiological and behavioral characteristics to identify an individual (Weber, 2006). A common theme in the definition is the recognition of identity based on individual properties. Such confirmation must be reliable for effective results.

Biometrics technology has now become the foundation of a wide range of collections of highly secured identification and verification mechanisms available for identity management. The contemporary meaning of biometrics technology emphasized the automated process (Lease, 2005). The aspect of automation has made rapid and large-scale deployment of the technology necessary.

Categories of biometrics. Biometrics is classified into two distinct areas: physiological and behavioral (Acharya, 2006; Bromba, 2007). Zorkadis and Donos (2004) stated that:

> Biometric technologies rely on who you are (physiological) or what you do (behavioral), as opposed to conventional methods, which rely on what you know (knowledge of passwords or other secrets such as cryptographic keys) and/or what you possess (such as a token or an ID card). (p. 125)

In Table 1**,** each category and related description is presented. Many adults will be familiar with one or two of these biometrics techniques (Weber, 2006). The reading of unique human physiological and/or behavioral attributes as data is a major functional advantage of the system (Short, 2002). The technology can be anything from access control to secured environment, change of password (Short, 2002), identification, or verification (Baird, 2002; Blackburn, 2004; Geising, 2003; Lease, 2005).

Table 1

Physiological and Behavioral Characteristics of Biometrics

Method	
Physiological	**Description**
Face recognition	Extracts key measurements from a digital image of the user's face and compares them with a stored 'faceprint'
Facial thermogram	Characterizes individuals by using varying temperatures emanating from different regions of the face
Fingerprint recognition	Assesses characteristic patterns of forks and ridges on the fingertips by using optical, capacitive, or thermal techniques to distinguish one person from another

(table continues)

Method	
Physiological	**Description**
Hand geometry	Measures the physical dimensions of the hand (for example, the span of the length of the fingers) when it is spread out on a flat surface
Iris scanning	Compares an image of the user's iris with a previously stored image
Retinal scanning	Scans the distinctive patterns on the retina
Vein checking	Assesses the characteristic vein patterns in the back of the hand by using infrared light
Behavioral	**Description**
Gait recognition	Characterizes individuals by the way in which they walk
Keystroke analysis	Monitors typing activity to determine characteristic rhythms; can be performed on the basis of known text (for example, in conjunction with a username and password) or keyboard inputs in general
Mouse dynamics	Monitors mouse-related activity and attempts to characterize users on the basis of measures such as speed and accuracy
Signature analysis	Assesses a handwritten signature that is captured using a special pen and/or pad: static analysis simply assesses the resulting pattern, whereas dynamic systems also measure the pressure and speed of the signature
Voice verification	Compares a user's voice with a previously stored 'voiceprint': can be performed on a text-dependent basis (that is, when speaking a known word or phrase) or text-independently

Note. From "Privacy Invasions: New technology that can identify anyone anywhere challenges how we balance individuals' privacy against public goals," By K. Weber, 2006, *European Molecular Biology Organization, Vol. 7 (Special Issue*), p. S37.

Properties of biometrics. Theoretically, any human physiological and/or behavioral characteristic can be used as a measure of biometric as long as it satisfied the following properties (Anonymous, 2007d; Bromba, 2007; European Commission, 2005; Jain, Ross, & Prabhakar, 2004; Lease, 2005; Woodward, Jr., Christopher, Gatune, & Thomas 2003; Zorkadis & Donos, 2004):

1. Universality: Each person should have the characteristic.
2. Distinctiveness: Any two persons should be sufficiently different in terms of the characteristic.
3. Permanence: The characteristic should be sufficiently invariant (with respect to the matching criterion) over a period of time.
4. Collectability: The characteristic can be measured quantitatively.
5. Performance: This refers to the achievable recognition accuracy and speed, the resources required to achieve the desired recognition accuracy and speed, as well as the operational and environmental factors that affect the accuracy and speed.
6. Acceptability: Indicates the extent to which people are willing to accept the use of a particular biometric identifier (characteristic) in their daily lives.
7. Circumvention: This reflects how easily the system can be fooled using fraudulent methods.
8. Measurable: The characteristics or trait can be easily presented to a sensor and the measurability allows for matching to occur in a matter of seconds and makes it an automated process.

9. Robustness: Refers to the extent to which the trait is subject to significant changes over time such as age, injury, and exposure to chemicals.
10. Comfort: Duration of verification and the ease of use.
11. Accuracy: Minimal error rates—clarity and consistency.
12. Availability: The portion of a potential user group who can use biometrics for technical identification purposes.

The seven pillars of biometrics technology. Although universality, distinctiveness, permanence, collectability, performance, acceptability, and resistance to circumvention are the properties, the European Commission differentiated these as the seven pillars of biometrics wisdom (European Commission, 2005). In Table 2, different types of biometrics modality and how each compared against the seven pillars is presented. The modalities discussed in this chapter, face recognition, iris identification, and fingerprint scan contrasted accordingly. For instance, the face recognition has high universality, collectability, and acceptability. In contrast, it has low distinctiveness, performance, circumvention, and medium permanence. The iris recognition has high universality, distinctiveness, permanence, performance, circumvention, low in acceptability, and medium in collectability. On the other hand, fingerprint scan has distinctiveness, permanence, performance, circumvention, medium in universality, and collectability respectively.

The seven pillars provide useful criteria for evaluating biometrics technology (European Commission, 2005; Jain, Bolle, & Pankanti, n.d.). They provide decision inputs to biometrics vendors for the manufacture of hardware and software applications. It is essential to note that the degree to which each biometrics technology fulfills a given

criterion will vary (European Commission, 2005). However, once particular application and identification objectives are determined, the seven pillars are important for comparisons to achieve better results.

The utilities of biometrics technology. Verification, watch-list, and identification are significant functions of biometrics technology (Archarya, 2006; Baird, 2002; Blackburn, 2004; Chirillo & Blaul, 2003; Geising, 2003; Lease, 2005; NSTC, 2006a; U. S. Treasury, 2005). In practice, biometrics technology is used in one of these areas:

1. Verification: Is the person who the individual claims to be?
2. Watch-list: Is this person in the database? If so, who is the person?
3. Identification: This person is in the database. How soon can the person be found? (Blackburn, 2004, n.p.)

Verification mode. The verification mode is the process of validating an individual's identity by comparing captured biometric data with the person's biometrics template stored in the system's database (Jain, Ross, & Prabhakar, 2004). The verification form is the basis for authentication systems (U. S. Treasury, 2005). In this type of approach, the system answers the question "Are you who you claim to be?" (Lease, 2005, p. 25) or "Is this X?" after the user claims to be X (Newton & Woodward, 2001, n.p.). The individual's claimed identity is either confirmed or denied (Geising, 2003) based on biometrics templates in the database.

Table 2

Comparison of Various Biometrics Technologies Against the Seven Pillars

Types of Biometrics	Universality	Distinctiveness	Permanence	Collectability	Performance	Acceptability	Circumvention
Face	High	Low	Medium	High	Low	High	Low
Fingerprint	Medium	High	High	Medium	High	Medium	High
Hand Geometry	Medium	Medium	Medium	High	Medium	Medium	Medium
Keystrokes	Low	Low	Low	Medium	Low	Medium	Medium
Hand Vein	Medium	Medium	Medium	Medium	Medium	Medium	High
Iris	High	High	High	Medium	High	Low	High
Retinal Scan	High	High	Medium	Low	High	Low	High
Signature	Low	Low	Low	High	Low	High	Low
Voice Print	Medium	Low	Low	Medium	Low	High	Low
Facial Thermograms	High	High	Low	High	Medium	High	High
Odor	High	High	High	Low	Low	Medium	Low
DNA	High	High	High	Low	High	Low	Low
Gait	Medium	Low	Low	High	Low	High	Medium
Ear	Medium	Medium	High	Medium	Medium	High	Medium

Note. From "Introduction to Biometrics," by A. K. Jain, R. Bolle, and S. Pankanti, n.d., p. 16.

A good example is verifying a user's identity prior to providing the user access to a computer account (Blackburn, 2004) or using an Automatic Teller Machine (ATM) for banking services such as deposit, withdrawal, fraud detection, prevention, and protection (Harris, 1999; Jain, Bolle, & Pankanti, n.d). If the system matches the individual correctly, this is known as correct verification and is referred to as a 1:1 (one-to-one) match (Blackburn, 2004; Geising, 2003; Lease, 2005). This operation may be performed quickly to generate *yes* or *no* results for decision making. Most biometrics technology devices operate in verification mode whereby the individual's claimed identity is validated through a comparison of captured biometrics characteristics with the person's biometrics template stored in the database (Geising, 2003). False verification occurs if the system fails to correctly match a claimed individual identity with the biometrics template of the person. This is referred to as incorrect verification (Blackburn, 2004).

Watch-list mode. The watch-list mode is the method of comparing a presented biometric against a smaller collection of reference biometrics (U. S. Treasury, 2005). The watch-list form of biometrics application is not commonly discussed in the literature, unlike the verification and identification functions. Usually, it is used in the surveillance of known criminals or suspects (Lewis, 2007) and determines if a person belonged to a watch-list of identities (Hong, Jain, Pankanti, Prabhakar, Ross, & Wayman, 2004).

In the context of both the global war on terror (GWOT) (Woodward, 2005) and larger national and homeland security issues both in the U. S. and internationally (Markowitz & Gravell, 2007), the watch-list technique was employed on several fronts, such as in airport security. "In the watch-list task, the biometric system determines if the individual's biometric signature matches a biometric signature of someone in the

database of the watch-list" (Blackburn, 2004, n.p.) This process is necessary for reliable verification and confirmation of the person.

The individual will not make an identity claim and might not personally interact with the system; for example, when someone compares "John Doe" in a hospital to a missing person database (Blackburn, 2004). The system will establish whether the biometric template of the person is in the database (Archarya, 2006) through a comparison and evaluation of similarity scores of an established watch-list threshold value (Blackburn, 2004). When a top match is obtained, it is known as correct detect and identify and often referred to as one-to-few matching (U. S. Treasury, 2005). This mode is referred to as screening watch-list and used in airport security, in public events, and surveillance applications (Hong, Jain, Pankanti, Prabhakar, Ross, & Wayman, 2004).

Identification mode. The identification process is an essential function of biometrics. Individuals must be recognized and reliably verified and given access and permission privileges. According to Shafir, "identification necessitates authentication" (2006, p. 3). The identification mode will recognize an individual by "searching the templates of all users in the database for a match" (Jain, Ross, & Prabhakar, 2004, p. 2). This is very important, particularly in the growing wave of identity fraud (Gordon & Wilcox, 2003), increasing global electronic commerce (Giesing, 2003), and the fight against GWOT (Woodward, 2005).

In the identification mode, the system conducts a 1: N (one-to-many) comparison to establish an individual's identity and fails if the subject is not enrolled in the database (Blackburn, 2004; Giesing, 2003; Lease, 2005). This is different from the verification mode of 1:1 (one-to-one) match system and the watch-list of one-to-few match systems.

Identification is a critical component during recognition where the system will establish either positive or negative identity (Jain, Ross, & Prabhakar, 2004; Lease, 2005; U. S. Treasury, 2005).

An important aspect of this process is the establishment of each individual's personality (Giesing, 2003). In practice, however, only a few applications claimed to offer biometrics identification utility (Blackburn, 2004) "whereby the individual submits a live sample and the system attempts to identify it within a database of templates" (Lease, 2003, p. 53). Scaling is a problem in this mode because if the system lacked sufficient throughput, it will affect system performance. This can lead to errors in the process and biometrics errors will raise concerns about false acceptance and rejection.

The faults associated with the technique are discussed later in this chapter. The identification mechanism has several advantages. According to Giesing (2003), the benefits are:

1. The cost of administration—faulty identity authentication results in unnecessary costs; however, biometrics identification can ensure accurate identity checking.
2. The integrity of identification—flawed identity-checking results in fraud and disrupts individual's services. Biometrics identification will ensure the integrity of the client's identity can be guaranteed.
3. The integrity of information—Biometrics identification can ensure that the correct information is linked to the right person.

4. Access to information in the organization's custody—Biometric identification enforces the need to know to allow only authorized personnel to gain access to organizational information assets.

5. The delivery of services and benefits—the speed of service delivery will lead to satisfactory customer service as a result of rapid identification of the correct individual. (p. 46)

Authentication mechanisms. Authentication is the process of proving the identity of an individual or a requester. The ability to establish recognition and validate and authorize users are very important in today's growing electronic age. "Sound identification and authorization mechanisms are often a necessary prerequisite for mitigating threats to other key security services such as confidentiality, non-repudiation, data integrity, and data availability" (Chandra & Calderon, 2003, p. 51).

Three types of authentication mechanisms are: knowledge-based, token-based, and biometrics authentication. Knowledge based is what a person knows, for example, a password. If a person had a smart card, on the other hand, then the technique is token-based. These two types of authentication mechanisms are vulnerable to breaches and can be compromised.

In contrast, biometrics technology prevents people from sharing, transferring, and exchanging their identity (AlBalawi, 2004). This is a major advantage that knowledge-based and token-based authentication mechanisms did not provide (Harris & Yen, 2002). Passwords and personal identification numbers (PINs) are easily shared to circumvent security policies. Table 3 shows current authentication mechanisms and their properties.

Table 3

Comparison of Current Authentication Techniques

Method	Examples	Properties
What you know	User ID Password PIN	Shared Many passwords are easy to guess Easily forgotten
What you have	Catch Badges Keys	Shared Can be duplicated Lost or stolen
What you know and have	ATM card and PIN	Shared Writing PIN on paper
Something unique about the user	Fingerprint Hand Iris Face Voice	Impossible to share Cannot be exchanged Repudiation Difficult to forge Cannot be lost or stolen

Note. From *Students' and Instructors' Attitudes Toward Using Biometric Technology as an Identification Method in Online Courses,* by W. AlBalawi, 2004, Unpublished dissertation, West Virginia University, Morgantown, p. 14.

The biometrics authentication process. Biometrics enrollment and verification modules provide a robust and streamlined process (AlBalawi, 2004; Blackburn, 2004; Brydie, 2008; European Commission, 2005; Hong, Yun, & Cho, 2005; RaviRaj Technologies, 2007; Ross, 2003; Wayman, 2000). During the enrollment phase, as shown in Figure 3, biometrics data of the user, such as the fingerprints, are acquired, captured, and processed through the sensor, quality component, and database (Brydie, 2008; Deschaine, 2005; Hong, Yun, & Cho, 2005; Jain, Ross, & Prabhakar, 2004; Lewis, 2007; Tilton, 2006).

Rand (2001) reported that biometrics system usually took three samples during the enrollment process and then computed the average. The resulting sample, which was measured, was converted using a proprietary algorithmic operation into a mathematical

representation, called reference or enrollment template. This stage will occur after determination that the system captured and recognized the data correctly for quality control and verification (European Commission, 2005).

The template, which is stored in a database, will be used to determine a biometric match (Deschaine, 2005), and establish identity (Lewis, 2007). When the user returns to the system, an analogous process to enrollment will occur. The user's relevant biometrics data will be extracted and then compared against the previously stored template in the database. If the score is within allowable or preset threshold criteria, the decision will be made either to match or not to match. Usually, the comparison was through the use of a Hamming Distance, (Khaw, 2002). Hamming distance is the process of contrasting of two binary data strings between current template and stored reference of biometrics in the database. The biometrics recognition/verification process is significant for the following reasons:

1. When two templates of biometrics are compared, they will be determined to have a level of similarity.
2. This signified a probability that both references came from the same person.
3. An evaluation was made in accordance with a preset decision threshold.
4. The declaration of a successful match or non-match was then made. (Deschaine, 2005; European Commission, 2005; Tilton, 2006)

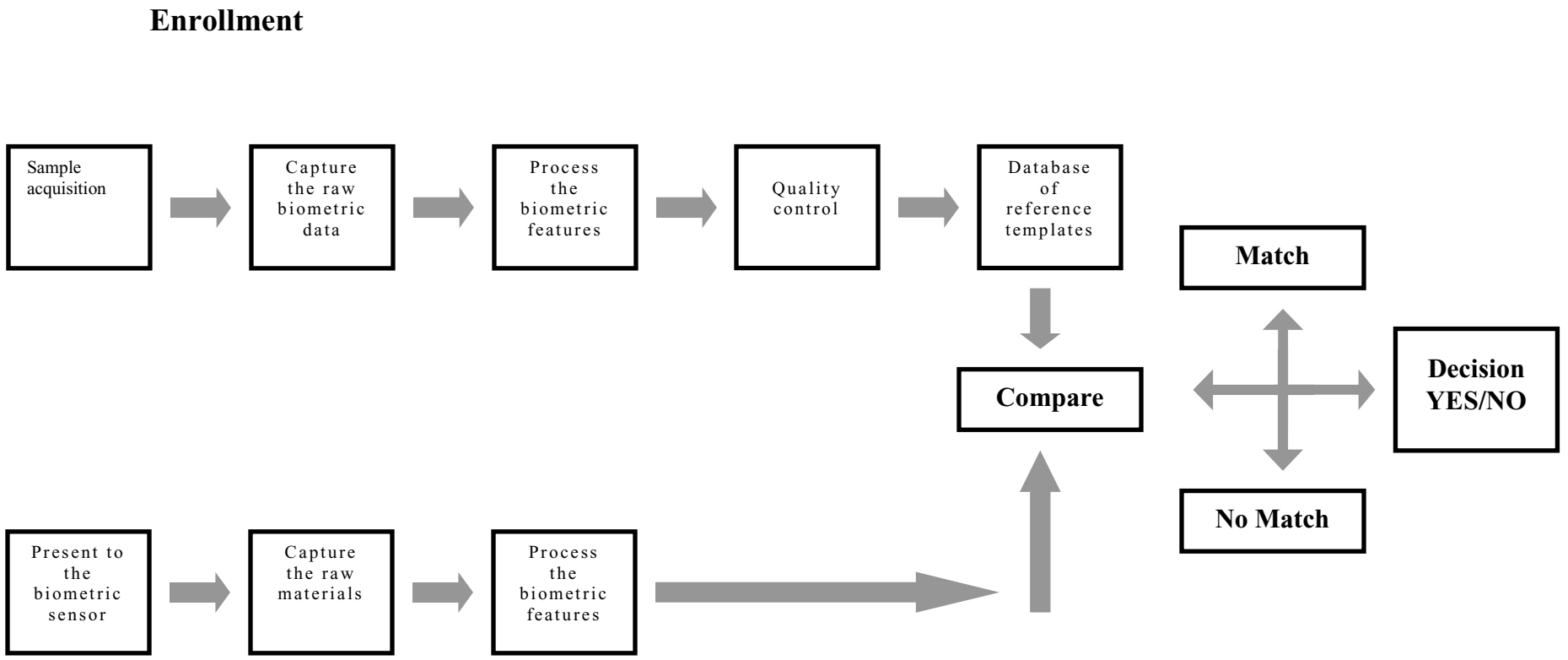


Figure 3. Core stages and modules in the authentication process of a generic biometrics system.

The implementation of biometrics recognition requires components such as capture devices that include dedicated hardware or sensors, a secure database for the acquired templates, and biometrics algorithms that will perform processing and matching operations (Tilton, 2006). The different components can be purchased separately or integrated with other electronic devices. For instance, a single-purpose fingerprint scanner can be developed and incorporated in personal digital assistants (PDAs), laptops, and cell phones (Tilton, 2006). The objectives to be accomplished are major factors in determining the type of biometrics system that will be implemented.

Advantages/Disadvantages of biometrics technology.

Advantages. Despite the criticisms of privacy advocates and Civil Libertarians as well as widespread public confusion "that biometrics will become a technology of surveillance and social control" (Cavoukian, 1999, p. 31), biometrics technology is gaining wider application and implementation. According to King, Lee, McKay, Marshall, Turban, & Viehland (2008, p. 528), "the worldwide focus on terrorism, and soaring fraud and identity theft" highlighted the need of using biometrics technology as control measures. Verifying identification, protecting identity, and detecting suspected terrorists are some of the primary benefits of biometrics technology. Other advantages of biometrics technology include:

1. Controlling access to sensitive facilities at airports for passengers' safety.
2. Preventing identity theft and fraud in the use of travel documents, stolen credit cards, and phony checks.

3. Identify known or suspected terrorists, e.g., a fingerprint was used to identify the 20th hijacker of the tragic event of September 11, 2001.
4. Increased security—provide a convenient and low-cost additional tier of security.
5. Employ hard-to-forge technologies and materials to reduce and control welfare fraud.
6. Eliminate problems caused by lost IDs or forgotten passwords.
7. Authenticate the user through behavioral and physiological traits, which are better than other methods of authentication such as token-based and knowledge based.
8. Reduce password administration costs.
9. Replace hard-to-remember passwords, which may be shared or observed.
10. Integrate a wide range of biometric solutions and technologies, customer applications, and databases into a robust and scalable control solution for facility and network access.
11. Make it possible, automatically, to know who did what, where, and when.
12. Offer significant cost savings or increasing return on investment (ROI) in areas such as loss prevention, time, and attendance.
13. Biometrics technology provides flexibility to operate either in identification or verification mode.
14. Unequivocally link an individual to a transaction or event.
15. Prevent fraudulent use of stolen cards, especially in conjunction with point-of-sale payments.

16. Biometrics technology serves as the gatekeeper of confidential personal data. (Barry 2002; Chirillo & Blaul, 2003; Jain, Ross, & Prabhakar, 2004; King, Lee, McKay, Marshall, Turban, & Viehland, 2008; Matyas & Riha, n.d; Nakashima, 2007; Questbiometrics, 2005; Woodward, 2001)

Disadvantages. Even though the need of biometrics technology is increasingly growing, there are concerns of balancing privacy, security, and liberty (PSL). If an individual's data are tagged with biometrics ID (Cavoukian, 1999), people will lose control of their identity. This means that preservation of personal privacy will be difficult. In addition, the cost of implementing the technology has raised concern. Other drawbacks reported in the literature included:

1. Biometrics technology is inherently individuating and it interfaces easily with database technology, making it easier to commit privacy violations.
2. Biometrics system is useless if there is no identified threat.
3. Biometrics is no substitute for quality data about potential risks.
4. Biometrics identification is only as good as the initial ID.
5. Biometrics identification is often overkill for the task at hand.
6. Some biometrics technologies are discriminatory.
7. It is impossible to assess the accuracy of biometric systems before deployment.
8. The cost of failure is high and might be consequential.
9. Performance is a big issue when the database is large.
10. The problems of accuracy and speed affect the system.

11. Biometrics data are not considered to be secret and the security of a biometric system cannot be based on the secrecy of user's biometric characteristics.
12. Biometrics system may be intrusive or personally invasive.
13. Lack of standardization and interoperability of vendor applications pose serious problems.
14. The loss of autonomy and anonymity if a biometrics template is stolen.
15. The concern of function creep—using the system beyond the original or stipulated intention.
16. Neither verification systems nor identification systems generate perfect matches.

(Abernathy, Tien, Granger, 2007; Electronic Frontier Foundation, 2006; Matyas & Riha, n.d.; Rosenzweig, Kochems, & Scwartz, 2004)

Types of biometrics technology. Several biometrics technologies are available commercially and others in development such as Odor sensing, Nailbed identification, and Skin pattern recognition (U.S. Treasury, 2005). Some of them that were deployed included signature, fingerprint, hand geometry, retina, iris, face, and voice (Allan, 2002, 2006; Archarya, 2006; Blackburn, 2004; Ruggles, 2002; U. S. Treasury, 2005). These are mainstream biometrics techniques (Archarya, 2006; Brydie, 2008; Chirillo & Blaul, 2003; European Commission, 2005; International Biometric Group [IBG], 2006, 2007; Lease, 2005; Liu & Silverman, 2001; Reedman, 2004; U. S. Treasury, 2005).

In research on biometrics, study respondents frequently mentioned the iris and the fingerprint. This researcher focused on face, iris, and fingerprint because each of these

has over 5% of the biometrics market share in 2007 compared to hand, 4.7%, voice, 3.2%, retina, signature, and other modalities 4% (IBG, 2007). An emphasis on fingerprint in this section indicated that it is widely adopted and accepted as the de facto international standard for positive and reliable verifications of identities (Chirillo & Blaul, 2003; Jamieson, Stephens, & Kumar, 2005).

Face recognition. The face recognition system extracts key measurements from a digital image of the user's face and compared them with a stored faceprint (Archarya, 2006; Weber, 2006; U. S. Treasury, 2005). Facial recognition is based on a computerized identification of unknown face images through comparison with a database of known images (Lease, 2005). The U.S. Treasury (2005) described face recognition as:

> The acquisition, segmenting, and matching of a given face against a database of faces—is a non-intrusive biometric method dating back to the 1960s. For over 30 years, the majority of work in face recognition has focused on use of two-dimensional images, using legacy data (e.g., drivers' licenses, criminal photographs) for matching of images. (p. 37)

According to Lease (2005), "face appearance is a particularly compelling biometric because it is one used every day by nearly everyone as the primary means for recognizing other humans" (p. 35). As a result of its naturalness, face recognition is more acceptable than other forms of biometrics modalities (Lease, 2005).

Face recognition is one of the fastest growing areas of the biometrics industry (Baird, 2002). Its growth was 11.4% in 2003 and 12.0% in 2004 (Lease, 2005; European Commission, 2005).The International Biometric Group stated that the growth of face

recognition in the biometrics industry was 12.9% in 2007 (IBG, 2007). This steady growth confirmed it to be the most frequently used biometric characteristic for everyday personal recognition (European Commission, 2005; Jain, Ross, & Prabhakar, 2004).

Despite the fact that face recognition is less accurate than fingerprints, nevertheless, it tends to be less invasive (U.S. Treasury, 2005), passive, and unobtrusive, and it can be extremely effective in scanning large crowds for known criminals and terrorists (Baird, 2002). It garnered headlines in January 2001, when it was used at the Super Bowl to scan the crowds for criminals. This led to the Super Bowl being dubbed the Snooper Bowl (Baird, 2002). Face recognition has several advantages and continues to draw mainstream recognition in the biometrics industry. The strengths of facial recognition include the following:

1. It uses standard video or still cameras and no physical contact is required.
2. It functions with existing databases, such as those used for police mug shots, motor vehicle registration, or passport photos.
3. Images can be captured from a distance without the subject's cooperation or even awareness.
4. It is easy to use and what is required is that the user (or target) looks at the camera.
5. It does not require the user to touch any device (a major objection for some users with finger scans and hand scans).

6. When deployed in verification situations, facial recognition systems have extremely low failure-to-enroll rates (unlike fingerprints, human faces are almost always distinctive).
7. The system captures faces of people in public areas, which minimizes legal concerns.
8. It integrates with existing surveillance systems that are in broad use. (Chirillo & Blaul, 2003; Lease, 2005; Nakashima, 2007; Woodward, Horn, Gatune, & Thomas, 2003)

The weaknesses of face recognition are the following:

1. Its accuracy is appallingly low, so it has a high error rate level.
2. Poor lighting, eyeglasses, facial hair, and facial expressions may affect performance.
3. The individual's appearance may change over time and affect operations.
4. In a large database search, there are many candidate matches that humans must examine.
5. Perceived threat to privacy: covertly deployed systems—such as those used for surveillance—pose significantly greater threats to privacy than the other top biometrics used in similar circumstance. (Lease, 2005; Nakashima, 2007)

Iris recognition. Iris recognition is the process of recognizing a person through the analysis of apparent patterns in the individual's iris (Ernst, 2002). The iris of an individual is absolutely unique. In the entire human population, no two irises were alike in their mathematical detail (Argus, 2007). The iris is the colored portion of a person's eye and a muscle within the eye that regulats the size of the pupil, controlling the amount of light that entered the eye (NSTC, 2006b).

The human iris continues to attract significant attention as a biometrics technique. The unique physiological patterns in the iris of the eye identify humans to a degree of accuracy that surpassed even DNA matching (Argus, 2007). The technique combines computer vision, pattern recognition, statistical inference, and optics. Its purpose is real-time, high-assurance recognition of a person's identity through mathematical analysis of the random patterns that are visible within the iris of an eye from some distance (Daugman, 1993).

The first step in iris recognition is to locate the iris using landmark features. These landmark features and the distinct shape of the iris itself allow for imaging, feature isolation, and image extraction. The system will then compare the unique characteristics of the iris, the colored area surrounding the pupil, to capture an iris image. Given the stable physical traits of the iris, this technology is considered to be one of the safest, fastest, and most accurate, noninvasive biometrics technologies (U. S. Treasury, 2005).

Its share of the biometrics market was 5.1% in 2007 (IBG, 2007). Iris recognition is forecast to play a role in a wide range of applications in the future as a person's identity must be established or confirmed (Daugman, 1993). The areas of application included

electronic commerce, information security, entitlements authorization, building entry, automobile ignition, forensic and police applications, network access and computer applications, or other transactions in which personal identifications currently relied on special possessions or secrets such as keys, cards, documents, passwords, and personal identification numbers (PINs) (Daugman, 1993). Other areas that iris recognition is used are in the military and law enforcement, transportation and border control, facility access, and airports (Daugman, 1993; European Commission, 2005; Nakashima, 2007). The implementation of iris identification as a security system has several benefits in identity management and restricting access to vital environments such as airports.

According to Lease, "The most important strength of iris biometrics is its accuracy, the most critical weakness of facial scanning. Of all the leading biometrics, iris technology has the lowest error rate and the highest level of overall accuracy" (2005, p. 41). Liu and Silverman (2001) also supported this position (see Table 5 in Section 5 of this chapter for a comparison of factors). Its contrast against the seven pillars of universality, distinctiveness, collectability, performance, and acceptability is outstanding (European Commission, 2005). Other strengths of iris biometrics technology are the following:

1. The ability to be used both for verification and identification.
2. It is very stable and generally remains so throughout the individual's lifetime.
3. It is relatively difficult to fake or spoof because it is an internal biometric.
4. Iris pattern characteristics are very unique and no two irises could be identical.
5. Many data points can be gathered in small templates (512K).
6. There may not be direct contact with a user, depending on the device.

7. It is considered friendlier than retina technology.
8. Iris technology can be used on networks for identification/authentication.
9. The cost of its application is less than retina technology.
10. Where enrollment is not a problem, iris recognition ensures security.
11. It works well through glasses or contacts and laser surgery does not affect it. (Chirillo & Blaul, 2003; European Commission, 2005; Lease, 2005; Nakashima, 2007).

The physiological properties of iris recognition are important for using it in identification, authentication, and watch-listing. As common with other security systems, there are drawbacks of iris technology. Eye diseases such as cataracts can decrease accuracy and high-quality photos of the iris may fool the sensors. The cost of iris technology is prohibitive compared to other forms of biometrics technology such as fingerprint, voice, face identification, and electronic signatures. Nonetheless, as the technology matures, the cost is expected to drop significantly. The lighting and other environmental conditions can affect image acquisition. As the iris is very small, it may be difficult to scan it from a distance. Additionally, the ability to enroll an individual to undergo the validation process will require cooperation. If the subject is un-cooperative, the result might not be reliable and may result in an error. The reliance of the technology on proprietary hardware and software is also a concern because this may affect interoperability and performance (Chirillo & Blaul, 2003; Lease, 2005; Nakashima, 2007; U. S. Treasury, 2005).

Fingerprint recognition. Fingerprint technique is one of the biometrics modalities significant in reliable recognition and confirmation of individuals. The technology has been in use for many decades. “Fingerprint identification has been used in law enforcement over the past 100 years and has become the de facto international standard for positive identification of individuals” (Jamieson, Stephens, & Kumar, 2005, p. 2).

Fingerprint recognition has one of the longest histories as the most extensively deployed biometrics technology in existence today (Lease, 2005; LogicaCMG, 2006; Rosenzweig, Kochems, & Schwartz, 2004; TRUSTe, 2005; U. S. Treasury, 2005). “It is probably the most widely used and well known biometric” (Rosenzweig, Kochems, & Schwartz, 2004, p. 3). Fingerprint scan is used to measure the ridge patterns of the fingertips (Nakashima, 2007).

A fingerprint image can be captured involuntarily or unconsciously (European Commission, 2005). Sometimes, people leave fingerprint trails on surfaces that they touch through the oil that coats the ridge of the print. The residue left behind is called a latent fingerprint. Such fingerprints can be enhanced using special powders and brushes and processed to be used for credentialing (U. S. Treasury, 2005). There are three major fingerprint types: arch, loop, and whorl (European Commission, 2005).

Fingerprint identification technology has benefited from technological advances and this has led to rapid, completely automated commercial fingerprint systems for verification (Archarya, 2006). For instance, the fingerprint systems that were used for large-scale identification utilizing “one-to-many” relationship required information from all 10 fingers rather than just one (Archarge, 2006). The improvement in fingerprint

technology led to the integrated, automated system that law enforcement agencies use today.

The Integrated Automated Fingerprint Identification System (IAFIS) that was operational in 1999 was a noteworthy development in biometrics industry (NSTC, 2006e). The IAFIS made fingerprint verification faster and dependable. The Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) maintains IAFIS. It contains the fingerprint and criminal history of over 47 million subjects in the Criminal Master File (European Commission, 2005; NSTC, 2006e) and is one of the largest biometrics databases in the world (European Commission, 2005). "The IAFIS provides automated fingerprint search capabilities, electronic image, storage, and electronic exchange of fingerprints and responses, 24 hours a day, 365 days a year" (European Commission, 2005, p. 137). It also reduced fingerprint search requests from three months to two hours for criminal inquiries and within 24 hours for civil queries (NSTC, 2006e).

Fingerprint identification has universal application; a misidentification rate of 1/1,000; and required medium security (Nyasulu & Fomene, 2001). Iris on the other hand, has a false reject probability rate of 1 in 11, 400 (Khaw, 2002). However, Liu and Silverman (2001) rated it high in terms of level of security. Jain, Bolle, and Pankanti (n.d) rated it high in uniqueness, permanence, and performance. It has been implemented extensively in crime investigation, identity verification, and fraud protection, and it is considered to be a matured biometrics technology. The extensive use of fingerprint verification mechanisms has been established (European Commission, 2005; Lease, 2005; Ross, 2003; U.S. Treasury, 2005; Woodward, Webb, Newton, Bradley, &

Reubenson, 2001; Woodward, 2005). As already stated, the 20th hijacker of the tragic event of September 11, 2001, was identified through a fingerprint technique (Woodward, 2005).

In 2004, fingerprint technology captured a 48% share of the biometrics market (Lease, 2005; European Commission, 2005). However, the International Biometric Group (2007) reported that the market share of the fingerprint was 25.3% in 2007, a decrease of 27.7%. This drop can be attributed to competing biometrics modalities such as face recognition (IBG, 2007) and emerging techniques such as vein scans and ear and facial thermography (U. S. Treasury, 2005). This drop notwithstanding, it is expected that the fingerprint technique will continue to maintain a dominant market position due to high accuracy and "a good balance related to the so-called seven pillars of biometrics" (European Commission, 2005, p. 136).

Advantages of fingerprint technology. The application and usability of fingerprint security system is growing due to the benefits. Fingerprint technology has matured and capable of reliable accuracy. Its strengths are the major reasons for wider deployment.

1. It is the most widely used biometrics technology and is ideal for access control to secured environments as well as computer networks.
2. Its high accuracy has been proven and documented.
3. Fingerprint technology has the capability to enroll multiple fingers.
4. Ease of use with limited training.
5. Some systems require little space for installation.

6. There are large amounts of existing data available to allow background and/or watch-list checks.
7. Proven successful in one-to-one verification and it is the leading biometric technology in revenue generation.
8. Has proven effective in many large-scale systems over several years of use.
9. It is a mature technology of identification.
10. Some fingerprint technology has a low cost for implementation.
11. Fingerprint identification is considered stronger than password.
12. There is a wide variety of application, depending on the manufacturer.
13. The availability of fingerprint scanning devices—though they may differ from manufacturer to vendor.
14. The immediacy of identification, thereby allowing speedy authentication.
15. Used for more than a century and has become the de facto international standard for positive identification of individuals. (Blackburn, Miles, & Wing, 2006; Chirillo & Blaul, 2003; European Commission, 2005; Jamieson, Stephens, & Kumar, 2005; Lease, 2005; U. S. Treasury, 2005)

Fingerprint identification is the oldest and most matured biometrics technology in use (Jamieson, Stephens, & Kumar, 2005). As a result, information is publicly available on how to circumvent it. The drawbacks of fingerprint technique are:

1. Fingerprint is easy to copy or reproduce, a situation called fake or dummy fingerprint.
2. Public concerns about privacy are paramount and legitimate as with other techniques.

3. The issue of functional creep where the finger scan data may be used for other purposes worry users and that is a major concern.
4. Health or societal concerns about touching a sensor that countless other individuals used. An individual's age and occupation may cause some difficulty in sensors capturing a complete and accurate image.
5. It is not easy to fix a fingerprint template if it is compromised.
6. The screens on fingerprint scanners tend to retain an obstructive buildup of oil and residue from user's fingertips.
7. Fingerprint scanning is not considered as secure as retinal or iris biometric technologies.
8. Fingerprint technology is obviously not appropriate for individuals that are missing hands or have hand deformation.
9. Deterioration of expected performance due to user's skin condition (dryness/moisture). (Blackburn, Miles & Wing, 2006; Chirillo & Blaul, 2003; Lease, 2005)

Fingerprint technology is extensively and increasingly used in diverse environments (Chirillo & Blaul, 2003; European Commission, 2005; Nakashima, 2007; U. S. Treasury, 2005).

Common application of fingerprint technology. The applications of fingerprint are in the following areas:

1. Network Access (non-mobile)
    a. Smart card

   b. E-commerce
   c. Sensing terminal
2. Mobile Access
   a. Cell phones
   b. Notebook (laptops)
   c. Portable Digital Assistants (PDAs)
3. Physical Access
   a. Door lock (Entrance control)
   b. Safe
   c. Other: Vehicles, Arms (RaviRaj Technologies, 2007)

In addition, fingerprint technology is currently used in conjunction with large central databases for forensics purposes, asylum requests (European Commission, 2005), and for checking entitlements. The demand, growth, and application of the fingerprint technique will continue to increase as security; identification, verification, authentication, cyber/Internet crimes, identity management, and the threat of global war on terror (GWOT) dominate the concerns of governments, industry experts, and the general public. The techniques this researcher discussed in this section are the mainstream biometrics modalities. There are other emerging techniques, which are discussed in the next section.

Emerging biometrics technologies. While the three modalities discussed above are the mainstream biometrics used to verify, identify, and watch-list individuals (Ngugi, 2005; NTSC, 2006; U. S. Treasury, 2005; Woodward, 2005), however, there are other biometrics techniques that are either deployed or under development. As the need to improve system efficiency, accuracy, and minimize costs as a substantial barrier, new modalities are emerging. For instance, vein recognition has been deployed but captured only 3% of the biometrics market and is not considered among the mainstream biometrics security systems. Other emerging biometrics techniques are: facial thermography, DNA matching, odor sensing, blood pulse measurement, skin pattern recognition, nailbed identification, gait recognition (capturing sequence of images), and ear shape recognition (U. S. Treasury, 2005). See Table 4 for information on how these work.

It is to be noted that DNA has been implemented in crime investigation and prosecution for several years but it is not yet regarded as biometrics technology (European Commission, 2005; Roethenbaugh, 1997). “In general DNA identification is not considered by many biometric recognition technology, mainly because it is not yet an automated process (it takes some hours to create a DNA fingerprint)” (European Commission, 2005, p. 147). The lack of automation in real time is a major concern (Roethenbaugh, 1997). This notwithstanding, DNA is extensively applied in crime inspection and trial and may emerge as a significant technique among existing biometrics technologies. In a comparison of various biometrics technologies against the seven pillars, DNA scored high in universality, uniqueness, permanence, and performance but

low in collectability and acceptability. The emerging biometrics technologies are presented in Table 4.

Biometrics performance: Types of errors and metrics. As the major biometrics systems are in use and other techniques continue to emerge, however, there are common errors. In this section, faults of the system are discussed. According to the U. S. Treasury (2005, p. 46), "Biometric system performance is not 100 percent accurate" and its performance is highly dependent on certain conditions and errors (European Commission, 2005). Errors plague the system such as false acceptance rate (FAR) and false rejection rate (FRR) (Acharya, 2006; Chirillo & Blaul, 2003; European Commission, 2005; Jain, Ross, & Prabhakar, 2004; Lease, 2005; Ruggles, 2002; U. S. Treasury, 2005; Woodard, 2004).

The false acceptance rate (FAR): this is the condition where biometrics measurements from two different individuals are identified as being from the same person (Acharya, 2006). In other words, it is the likelihood that a biometrics system will incorrectly identify an individual or fail to reject an impostor (Woodward, 2004). It is also known as false match rate (FMR) and is expressed in percentage. Woodard (2004) stated that the false acceptance rate may be estimated as follows:

FAR = NFA/NIIA or FAR = NFA/NIVA where

FAR is the false acceptance rate

NFA is the number of false acceptances

NIIA is the number of impostor identification attempts

Table 4

Emerging Biometrics Technologies

Biometrics Type	How It Works	Maturity
Vein scan	Captures images of blood vessel patterns	Commercially available
Facial thermography	Infrared camera detects heat patterns created by the branching of blood vessels and emitted from the skin	Initial commercialization attempts failed because of high cost
DNA matching	Compares accrual samples of DNA rather than templates generated from samples	Many years from implementation
Odor sensing	Captures the volatile chemicals that the skin's pores emit	Years away from commercial release
Blood pulse measurement	Infrared sensors measure blood pulse on a finger	Experimental
Skin pattern recognition	Extracts distinct optical patterns by spectroscopic measurement of light scattered by the skin	Emerging
Nailbed identification	An interferometer detects phase changes in back-scattered light shone on the fingernail; reconstructs distinct dimensions of the nailbed and generates a one-dimensional map	Emerging
Gait recognition	Captures a sequence of images to derive and analyze motion characteristics	Emerging; requires further development
Ear shape recognition	Is based on distinctive ear shape and the structure of the cartilaginous, projecting portion of the outer ear	Still a research topic

Note. From "The Use of Technology to Combat Identity Theft," *Report on the Study Conducted Pursuant to Section 157 of the Fair and Accurate Credit Transactions Act of 2003,* U. S. Treasury, 2005, Washington, DC: General Accounting Office, p. 42.

NIVA is the number of impostor verification attempts

NIR is the number of impostors rejected (p. 3).

Roethenbaugh (1997) expressed the rate as percentage in the following formula: FAR: NFA/NIR x 100 (p. 7).

The false rejection rate (FRR), also known as the false non-match rate (FNMR), is an error that occurs when a biometrics system falsely rejects an authorized individual (Chirillo & Blaul, 2003; Lease, 2005; Woodard, 2004). According to Woodard (2004), the false rejection rate may be computed as follows:

FRR = NFR/NEIA or FRR = NFR/NEVA where

FRR is the false rejection rate

NFR is the number of false rejections

NEIA is the number of enrollee identification attempts

NEVA is the number of enrollee verification attempts (p. 3)

This is expressed in percentage according to this formula: FRR: NFR/NEVA x100 (Roethenbaugh, 1997, p. 7).

The crossover error rate (CER) (Chirillo & Blaul, 2003; Hong, Yun, & Cho, 2005; U. S. Treasury, 2005) also known as equal error rate (EER) (Acharya, 2006; Lease, 2005) is an important metric in biometrics technology systems. It occurs "when the decision threshold of a system is set so that the proportion of false rejections will be approximately equal to the proportion of false acceptances" (Woodard, 2004, p. 2). At this juncture, the total rejected is equal to the number accepted. "The lower the CER, the more accurate and reliable the biometric device" (Liu & Silverman, 2001, p. 27).

Conversely, the higher the crossover error rate, the less correct and the more unreliable the system is.

The failure to enroll (FTE) is another critical metric of biometrics technology. This is a condition whereby an individual cannot enroll biometrics to create a suitable quality for subsequent automated operations (Lease, 2005). An individual's physiological and behavioral traits can present barriers to enrollment and therefore will affect error conditions.

Biometrics errors are not easy to eliminate (AlBalawi, 2006), but the type of biometrics trait used will influence either the FAR or FRR. For instance, fingerprint, iris, and dynamic signature will produce "lowest FARs at a rate of 1 in 10,000 or better" (AlBalawi, 2006, p. 15). In contrast, voice recognition, hand geometry, and facial recognition have high FAR rates. The design and performance of a biometrics system will impact accuracy and fault rates. This will occur if the technology is not properly evaluated (Archarya, 2006; Hong, Yun & Cho, 2005). The technology sellers, dealers, and merchants will influenc the fault rates. For instance, Roethenbaugh (1997) explained that "a biometric vendor can alter the systems FAR so that these rates can be achieved. However, to do this, the false rejection rate will suffer as a consequence" (p. 7) and this will affect reliability and functionality.

There is confusion in the descriptions of the terminologies associated with these errors. In some of the literature, the use of "False Match Rate" and "False Non-Match Rate" are often synonymous with "False Acceptance Rate" and "False Rejection Rate" (U. S. Treasury, 2005, p. 48). The national and international bodies are making efforts to standardize these terms and minimize ambiguities and improve the understanding of

them. These international bodies are the International Organization for Standardization and the International Electro technical Commission that established a Joint Technical Committee 1 (ISO/IEC JTC 1) (Tiresias, 2008), and the International Committee for Information Technology Standards (INCITS). In the section, the controversy surrounding biometrics is presented.

Part 4: Criticisms of Biometrics

There are considerable criticisms surrounding biometrics. Despite important benefits over prior security measures and comparable technologies, there are issues and concerns. Many people realized the significant advantages as the technology has improved and used for monitoring and controlling identity (Bocozk, Buster, Fitzgerald III, Vacca, Welsh, & Wulf, 2005). A major negative concern is tracking. According to Electronic Frontier Foundation (2007):

> By far the most significant negative aspect of biometric ID systems is their potential to locate and track people physically. While many surveillance systems seek to locate and track, biometric systems present the greatest danger precisely because they promise extremely high accuracy. (p. 4)

The other controversy surrounding biometrics is the loss of privacy (Archarya, 2006; Baird, 2002; Cavoukian, 1999; European Commission, 2005; Jain, Ross, & Prabhakar, 2004; Jain, Bolle, & Pankanti, n.d; Newton & Woodward, 2001; NSTC, 2006d; Vollmer, 2006). As the rate of global implementation and adoption of biometrics systems increased, the concern that privacy and individual rights were invaded increased. "In the United States, the freedom of the individual is perceived to be closely related to

his ability to operate somewhat autonomously and anonymously in the eyes of the state as well as other organizations" (Woodward, Webb, Newton, Bradley, & Rubenson, 2001, p. 22) that collected data from individuals without permission.

Privacy is what individuals do in their own space where they determined how and with whom to interact "either with trust, openness and sense of freedom, or with distrust, fear and a sense of insecurity" (Cavoukian, 1999, p. 29). Furthermore, privacy is where the individual's interest and autonomy that usually will arise as an assertion against other people or organizations are threatened (NSTC, 2006d). Privacy advocates have raised concerns that biometrics technology will invade confidentiality and violate individual rights (Vollmer, 2006). On the other hand, biometrics is not inherently good or bad for privacy but can impact individual rights based on how it is designed, developed, and deployed (Pilgrim, 2007). Privacy apprehension was one of the significant problems confronting not only the biometrics industry but also any organization that gathered personal information (ANSI, 2005).

Key apprehensions of privacy issues related to the data subject, the individual, or the organization that gathered biometrics data. Perhaps the increasing discussions of privacy issues focused on individuals because users have no control over the distribution of their data and were wary of data misuse (Allan, 2002). Tiresias (2008) characterized different forms of privacy as:

> Privacy Protective: A privacy-protective system is one used to protect or limit access to personal information, or which provides a means for an individual to establish a trusted identity.

> Privacy Sympathetic: A privacy-sympathetic system is one that limits access to and usage of personal data and in which decisions regarding design issues such as storage and transmission of biometric data are informed, if not driven, by privacy concerns.
>
> Privacy Neutral: A privacy-neutral system is one in which privacy is not an issue, or in which the potential privacy impact is slight. Privacy-neutral systems are difficult to misuse from a privacy perspective but do not have the capability to protect personal privacy.
>
> Privacy Invasive: A privacy-invasive system facilitates or enables the usage of personal data in a fashion inconsistent with generally accepted privacy principles. (p. 8)

Despite the increasing concern of privacy, another debate over the adoption of biometrics is about physical privacy that focused on user freedoms and continue to raise greater anxiety of the state watching (Archarya, 2005; ANSI, 2005; Rand, 2001; Woodward, Webb, Newton, Bradley & Rubenson, 2001). Privacy advocates object to the use of biometrics and other verification tools for collecting individual's information for fear of having a " 'surveillance society' in which governments and private corporations were collecting increasing amounts of personal data, sometimes without justification" (Archarya, 2005, p. 8).

Such a situation is dubbed "Big Brother" and is a social control mechanism (Archarya, 2005; Cavoukian, 1999; Lease, 2005). ANSI (2005) and Woodward et al. (2001), on the other hand, elevated the trepidation of physical privacy that included stigmatization, actual harm, and hygiene. An example of stigmatization is the association

of fingerprinting with criminal activity (ANSI, 2005; Woodward et al., 2001). Another major criticism and disapproval of biometrics is referred to as function creep (Archarya, 2005; ANSI, 2005; Lease, 2005; Liu, 2008; Mordini & Petrini, 2007; Pilgrim, 2007). This will occur when the data collected for one specific purpose is subsequently used for another unintended exploit without justification or authorization of the data subjects (Archarya, 2005). This violated accepted privacy principles (Tiresias, 2008). Lease (2005) cited a typical example of function creep in the following instance:

> The classic example of function creep is the use of the Social Security Number (SSN) ... the original Social Security cards containing the SSN bore the legend, "Not for Identification"... By 1961, the IRS began using the SSN for tax identification purposes. By 2002, countless transactions from credit to employment to insurance to many states' drivers licenses require a Social Security Number and countless private organizations ask for it even when it is not needed specifically for the transaction at hand. (p. 57)

Today, social security numbers are stolen and used to commit criminal activities such as identity fraud.

Other controversial concerns surrounding biometrics are the collection of data catalogued (Watkins, 2007). Humans see this as the mere reduction of individuals as identifiers that can be associated to commit crimes. It is difficult to easily substitute biometric data compared to credit card (Watkins, 2007). Once the digital identifier is breached, it is not possible to use it for identification, authentication, and comparisons of records in the central database. The automation of recognition is another controversy of the technology (Watkins, 2007). The reason to automate the process is to avoid human

errors. If the system fails, who will be responsible to correct the mistakes? It must be realized that the cost might be consequential.

The growing health concern is another cause of apprehension. Users have raised the anxiety of the cleanliness of sensors used to capture data from fingerprint, iris, and facial scans (Bocozk, Buster, Fitzgerald III, Vacca, Welsh, & Wulf, 2005). Although there is no report that confirmed any health issue associated with biometrics, however, this can instill fear on users and discourage them from biometrics enrollment and verification process.

Such concern really merited further investigation from health professionals, vendors, and biometrics subject experts. The religious objection can arise from different groups. This is particularly necessary due to legal and societal emphasis of respect on religious beliefs (Bocozk et al, 2005). These controversies notwithstanding, (Lease, 2005) further stated that "supporters of biometric authentication systems argue that properly deployed and with adequate best practice controls, biometric systems can actually function to enhance and protect privacy" (p. 57).

It is important to recognize the need for privacy principles, formulate, and align capability with an intention to protect users from unauthorized intrusion. Biometrics experts claimed that the potential application of the technology is tremendous. Its use and, consequently, its acceptance is inevitable (Cavoukian, 1999). However, as governments continued to adopt and rapidly implement the technology, the privacy of the individual has been threatened (Vollmer, 2006). It is, therefore, necessary to implement protective safeguards in conjunction with the technology so that public safety and protection are maximized while the intrusion of individual's privacy is minimized

(Vollmer, 2006). This will avoid the anxiety of stigmatization. Still, the protection of personal privacy will partly depend on system design, implementation, training, and usability.

Businesses will need to accept the responsibility to protect customer data and, therefore, privacy. "To appropriately and effectively balance the use of biometric information for legitimate business purposes with the customer's right to privacy, companies should adopt and implement the fair information practices and requirements" (Cavoukian, 1999, p. 44). Some of the fair information practices and requirements are to minimize or avoid unauthorized data collection, unnecessary/unreasonable collection of data, unauthorized use, and unauthorized disclosure (Cavoukian, 1999).

Contrary to Cavoukian's stated position, ANSI (2005) offered the solution of biometrics application through privacy enhancing technologies (PETs). These are coherent systems of information and communication technology (ICT) measures that protected privacy through an elimination or reduction of personal data or through prevention of unnecessary and/or undesired processing of personal data—all without losing the functionality of the data system.

Technology is not foolproof and using biometrics to verify and identify individuals will continue to cause public outcry from privacy watchdogs. It is important, therefore, that safeguards are incorporated and that organizations implemented sufficient privacy principles to protect individual's security and minimize the compromise of customer data. This will give subjects the assurance that information about them are controlled and protected and not sold to third-party vendors as data aggregates or stolen

to be used in criminal activities. The public will trust organizations with their data and the system will be seen as enhancing security and protecting privacy.

Part 5: Biometrics Adoption and the Technology Acceptance Model (TAM)

Several factors affected the adoption and acceptance of biometrics system. Liu and Silverman (2001) claimed that error incidence, accuracy, cost, user acceptance, required security level, and long-term stability were among the reasons biometrics systems were either adopted or not. Similarly, (Rajchel, 2007) wrote that the lifecycle of the system, invasiveness, health and hygiene, religion, ethic, and culture will affect adoption. Table 5 shows a comparison of different factors influencing the adoption of mainstream biometrics technology (Liu & Silverman, 2001). The technology acceptance model (TAM) is another important aspect of implementation that has significant contribution towards biometrics adoption. There are differing viewpoints according to the authors and the model; however, there are some overlaps of several reasons influencing the adoption of biometrics technique. It is therefore necessary to analyze these views relative to the need and the decision to adopt, availability of experienced personnel, financial resources, and the type of biometrics technology for adoption and implementation.

Table 5

Comparison of Factors Influencing Biometrics Adoption

Characteristic	Fingerprints	Hand geometry	Retina	Iris	Face	Signature	Voice
Ease of Use	High	High	Low	Medium	Medium	High	High
Error incidence	Dryness, dirt, age	Hand injury, age	Glasses	Poor lighting	Lighting, age, glasses, hair	Changing signatures	Noise, colds, weather
Accuracy	High	High	Very high	Very high	High	High	High
Cost	*	*	*	*	*	*	*
User acceptance	Medium	Medium	Medium	Medium	Medium	Very high	High
Required security level	High	Medium	High	Very high	Medium	Medium	Medium
Long-term stability	High	Medium	High	Higher	Medium	Medium	Medium

***** The large number of factors involved makes a simple cost comparison impractical.

Note. From "A Practical Guide to Biometric Security Technology," by S. Liu, and M. Silverman, 2001 (January/February), *IT Professional*, *3*(1), p. 31.

The Technology Acceptance Model (TAM). The technology acceptance model is a theoretical framework in helping to understand how perceived usefulness and perceived ease of use will affect adults' behavior toward the adoption and use of technology (Klopping & McKinney, 2004; Ngugi, 2005; Wahid, 2007). Understanding the factors that will affect implementation of technological systems had the potential to improve the design, adoption strategies, (Shen, Laffey, Lin, & Huang, 2006), and user acceptance (Davis, 1993). Ngugi (2005) argued that it "is probably the most popular model in the technology acceptance literature" (p. 49). There are greater interest and support for TAM due to its accumulated empirical strength to clarify the constructs that influenced acceptance of technology within organizational contexts (Mahinda & Whitworth, 2005). The model has been referenced extensively in the literature.

The constructs of perceived usefulness, perceived ease of use, and subjective norm have been used to explain technology adoption, usage, and acceptance (Shen, Laffey, Lin, & Huang, 2006). The authors postulated that perceived usefulness (PU) and perceived ease of use (PEOU) affected attitudes and behavioral intentions toward using new technologies such as biometrics technology. For example, users must believe that the technology will be easy to use, useful for reliably identifying people, and controlling deception and that it will enhance personal security.

These beliefs will generate attitudinal or behavioral intentions and interests to use the technology. Unless there is a problem, this will lead to the actual use of a biometrics system. Alternatively, if users believed that the system is complex and did not provide reliable performance, then the behaviors toward the system will be negative, which will

impact adoption. It is to be noted, however, that external variables such as the characteristics of the system design, available training, awareness, interest, and documentation will also impact technology usage (Wahid, 2007).

Despite how successfully TAM can be employed to explain factors that will influenc adoption of various technologies, expert designers find it difficult to operationalize the model at the implementation level (Ngugi, 2005). It is deficient in criteria such as flexibility, reliability, and extendibility (Mahinda & Whitworth, 2005). The model has been further criticized as being incomplete since it did not take into account other influences such as security, privacy, and trust, which also influence adoption (Brydie, 2008; Joshua & Koshy 2009; Shen, Laffey, Lin, & Huang, 2006).

In a study that Joshua and Koshy (2009) conducted, these authors concluded that perceived ease of use and the security helped to determine attitudes toward the acceptance of technological systems. Kim (2006) found that physical security is a factor that affected acceptance of the system by hotel guests, while trust and reliability were stated as reasons for adoption in a study that Brydie (2008) conducted. The knowledge of the factors that affects execution of technological systems will improve the design and adoption strategies (Shen, Laffey, Lin, & Huang, 2006), and user acceptance (Wahid, 2007).

The model in Figure 4 shows the relationship between ease of use, usefulness, and security and attitude formation and intention toward acceptance of biometrics technology (Joshua & Koshy, 2009). The original model that Davis (1993) developed did not include security as a construct. Through the years, researchers argued that other factors will affect the attitudinal and behavioral intentions to use technology besides perceived ease of use

and perceived usefulness (Cowen, 2009; Joshua & Koshy, 2009; Jahangir & Begum, 2008; Shen, Laffey, Lin, & Huang, 2006). Such factors may include security, awareness, and interest.

Ease of use. The first construct of TAM is ease of use. Researchers claimed that perceived ease of use was the extent of the individual's acceptance as true that there was no cost associated with using an exact method (Jahangir & Begum, 2008; Joshua & Koshy, 2009). Perceived ease of use was the user's awareness that the use of biometrics will involve minimal effort. According to Jahangir and Begum (2008), "understanding the technology leads to adaptation" (p. 34) and this is very important of forming a positive attitude toward acceptance of the system.

Perceived usefulness. The importance of perceived usefulness has been recognized in the banking industry (Jahangir & Begum, 2008; Joshua & Koshy, 2009), information technology sectors (Davis, 1999, 2001), and in educational course delivery systems (Shen, Laffey, Lin, & Huang, 2006).

Perceived usefulness is the second construct of TAM and has been referenced in numerous studies (Joshua & Koshy, 2009) for adoption of technology. Jahangir and Begum (2008) stated that, "perceived usefulness refers to consumer's perceptions regarding the outcome of the experience" (p. 33). It is a major determinant of actual behavior, which will encourage user behavior in twenty-first century transactions (Jahangir & Begum, 2008). If adults will believe that biometrics system is helpful and effective to protect individual security, privacy, and control of identity fraud, they will accept its use. On the other hand, if they did not realize the usefulness, that will affect the adoption.

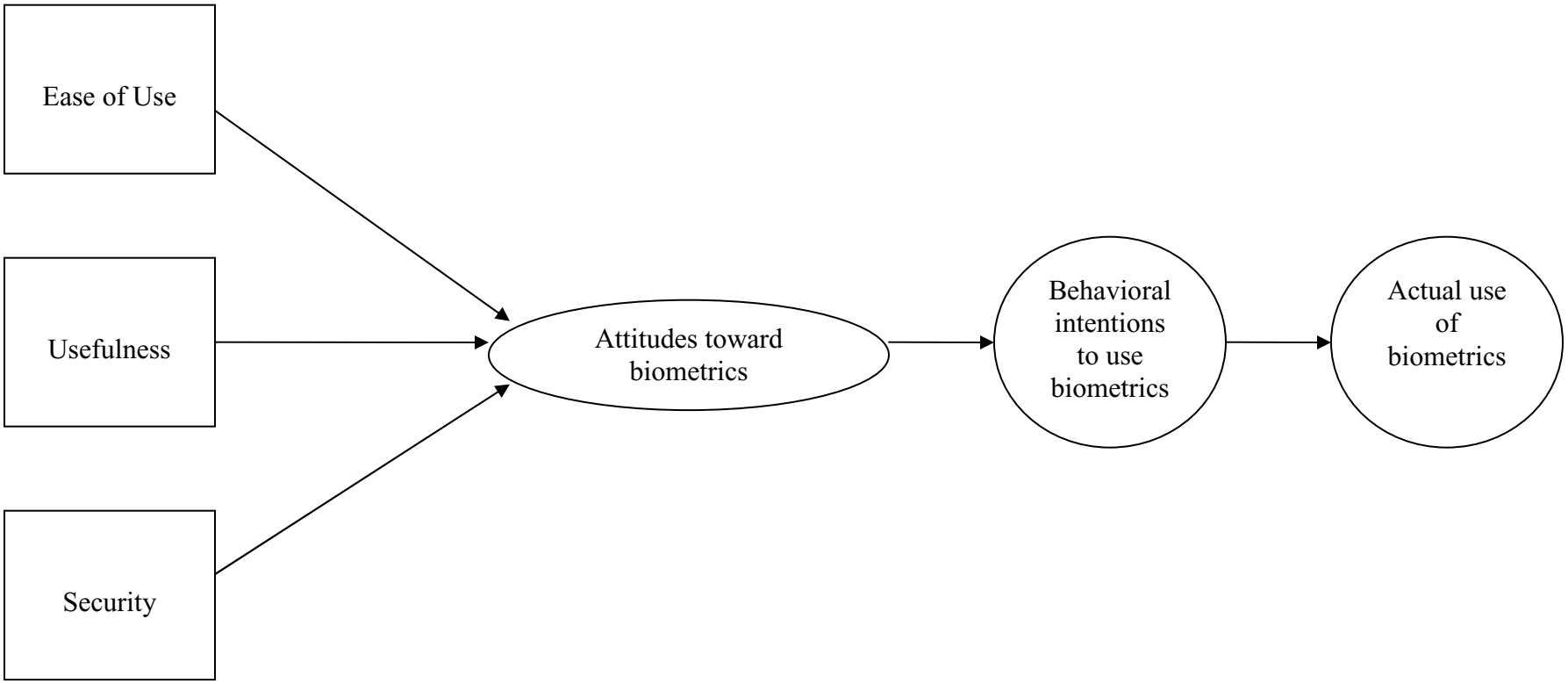


Figure 4. Technology Acceptance Model.

Security. Security is a significant concern for individuals (Jahangir & Begum, 2008). The need to protect identity and prevent self-deception is necessary for avoiding risks. When users perceive sufficient security and reliability in the use of technology, their attitudes toward the system will be positive. This would encourage the use of biometrics. Likewise, there is a sense of loss of safety if the system did not protect people or reliably recognize them.

Prior studies have concentrated on these two constructs of TAM: perceived ease of use and perceived usefulness. However, security is included as the third construct to explore its influence on adult behaviors toward biometrics system adoption.

Awareness. Regardless of accessibility, the possibility of encouraging the use and adoption of biometrics is significantly reduced without awareness (Asfaw, 2006; Norris, 2001). The awareness level of the technology will impact implementation depending on the age group. These key areas will play important roles in the adoption, implementation, and usability:

- Awareness of the ways in which biometrics can be used throughout daily life,
- Awareness of access, availability, and
- Awareness of the effects and benefits of biometrics technology to combat fraud and identity management.

Although high awareness levels may not necessarily translate into adoption and usability of biometrics, however, its function to impact acceptance is very important on the long run. It is, therefore, essential to note that an individual could be totally aware of

the existence of biometrics technology while possessing minimal knowledge surrounding its availability, purpose, effects, and usefulness. Over time, the awareness is expected to bring change in behavior and attitude toward acceptance of biometrics technology and the factors that underlie implementation.

Attitude. Alrafi (2005) wrote that attitude is "considered socially significant in the individual's society" (p. 4). It is believed to be a disposition that is necessary for evaluating behaviors in different ways. The behavioral conduct can be negative or positive. According to Alrafi (2005), an attitude is:

1. an implicit response,
2. which is both (a) anticipatory and (b) mediating in reference to patterns of overt responses,
3. which is evoked (a) by a variety of stimulus patterns (b) as a result of previous learning or of gradients of generalization and discrimination,
4. which is self-cue and drive-producing,
5. and which is considered socially significant in the individual's society. (p. 4)

The relationship between attitude and behavior is quite clear. An individual that has a positive impression of the technology will develop an affirmative attitude.

Conversely, a disapproving feeling will translate into a negative mindset toward the system. However, adult users will form opinions and behave either positively or negatively toward biometrics system based on their perceived ease of use, perceived usefulness, and security (Joshua & Koshy, 2009; Jahangir & Begum, 2008). Other factors

that will influenc technology adoption are awareness and level of interest (Gaudin, 2003; Mansfield, 2009; Norris, 2001).

Part 6: Identity Fraud

In this review, it is important to discuss identity fraud and the increase in concerns about its consequences. Identity fraud (IDF) is the unauthorized use of personal and financial identifiers to commit crimes (Choo, Gordon, Gordon, & Rebovich, 2007). The prevalence of identity fraud is growing into a national and global crisis (Gordon & Willox, 2003, 2006; Oghre, 2007), which will facilitate other crimes (Choo, Gordon, Gordon, & Rebovich, 2007). The rate of identity deception and the costs to the victims and the public are enormous (Gordon & Willox, 2003). The costs to people who suffered identity fraud reached $48 billion in 2008 (Stampel, 2009). This is alarming. In recent years, the issue of maintaining personal security received heightened attention (Newman & McNally, 2005) and this is expected to continue.

Studies and reports that addressed the relationship between identity fraud and biometrics technology have significantly enhanced the understanding of the role of biometrics to protect identity and maintain individual security. In reviewing the literature, there is an increase in favorable views toward the application of biometrics techniques to control identity deception in advanced countries. An unresolved and important question with regard to this research is: What are the important reasons that will impact adults' acceptance of biometrics system in developing countries, such as Nigeria? This study explored the increasing trend of identity fraud in Nigeria and the relationship between

adult attitudes toward the factors that will influence the adoption of biometrics technology for identity management. In Figure 5, the process of IDF is presented.

There has been a dramatic increase in the types of methods criminals used and obtained personal identifiers from databases (Gordon & Willox, 2006; Newman & McNally, 2005). These included logging programs and a variety of other techniques to access databases that contained vast personal information. Newman and McNally (2005) reported four sources of available information that increased identity fraud: "public databases (records of birth, marriage, tax records, etc.), commercial databases (energy or telephone bills, mortgage papers), professional, and employment history (school or university, educational degrees), and family records (family, referees, parents or guardians" (p. 39). Several documents are derived from these sources.

Usually, these documents are easily acquired through fictitious identifiers or they are stolen (Gordon & Willox, 2003). These will provide access to a breeder record such as a birth certificate, which will allow for the procurement of other documents such as driver's license, passport, and social security card. From these, a credible identity is created to provide access for employment, credit cards, bank accounts, secure facilities, computer systems, leases, and mortgages (Gordon & Willox, 2003). The procurement of these records will further facilitate activities for profits and the commission of financial crimes, terrorism, money laundering, drug trafficking, and weapons smuggling (Gordon & Willox, 2003; Norman & Thomas, 2005).

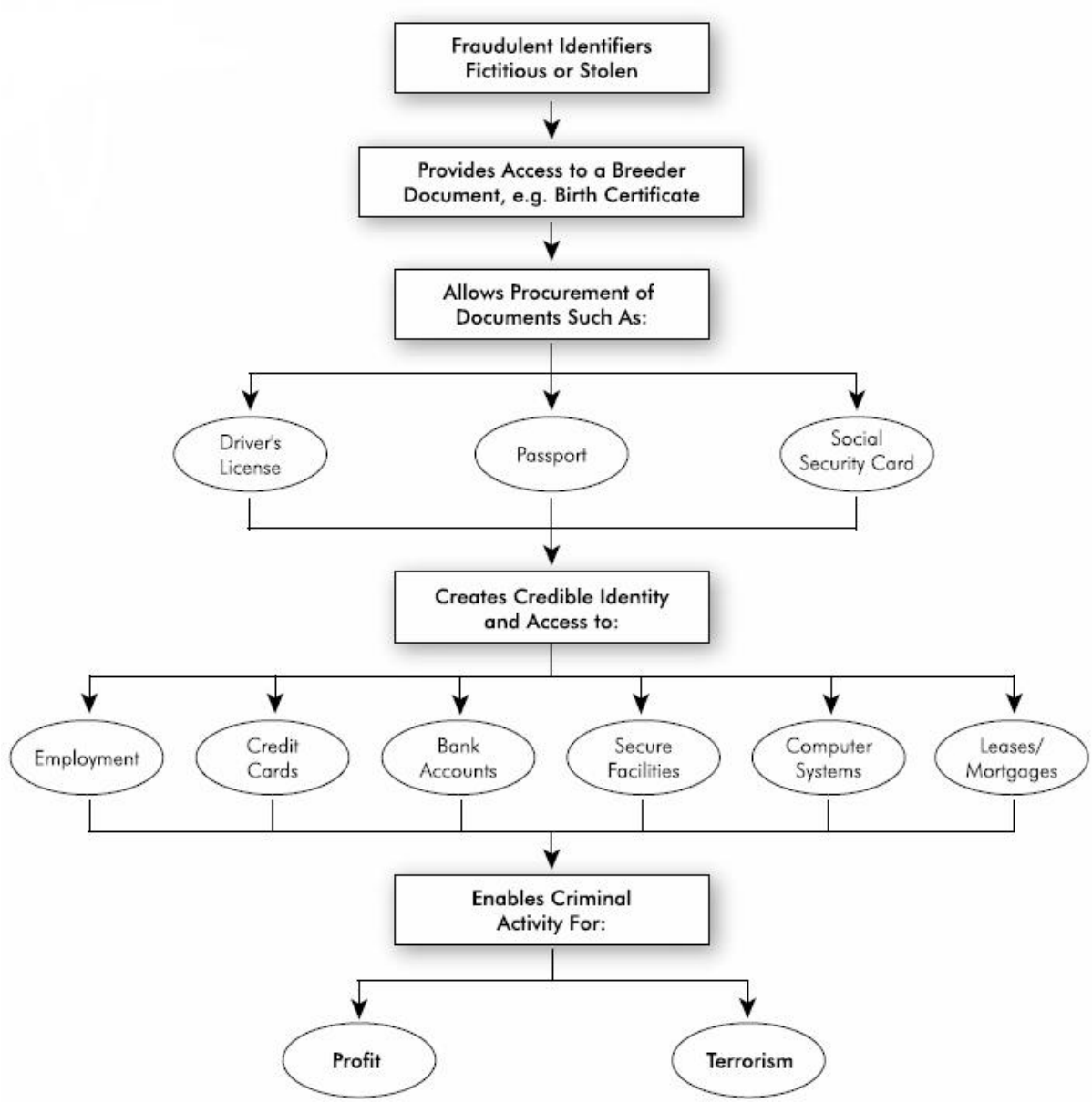


Figure 5. The Identity Fraud (IDF) Process. From Identity Fraud: A Critical National and Global Threat, by Gordon and Willox, 2003, Economic Crime Institute, Utica: New York, p. 19.

These criminal actions threatened personal and national security, global commerce, economic activities, and the stability of democracies. Kristin and Erin (2001) stated that "identity fraud is the fastest growing white-collar crime in the United States" (p. 1). Kristin and Erin reported two identity fraud rings the police disrupted in Detroit and in Queens, New York. For instance, in the New York ID fraud ring, dubbed *Nigerian Express*, the criminals made 113 banking transactions and transferred over $1.4 million—although law enforcement officers estimated that actual losses were more than that (Kristin & Erin, 2001). In another case, a Nigerian citizen was sentenced for ID fraud after being convicted of using other people's social security numbers and identification information to obtain credit cards and bank cards in the name of the victims by assuming their identity (Brackin, 2005).

Some of the 9/11 hijackers applied extensive use of ID fraud processes and legitimized their identity (Norman & Thomas, 2005). Two of the terrorists, Abdul Azziz Alomari and Ahmed Saleh Alghamdi, who lived in Maryland motels, falsified their records and obtained Virginia state identification documents. They used the documents and boarded the ill-fated planes of the September 11, 2001 attacks (Norman & Thomas, 2005). This demonstrated a classic example of identity deception in the commission of a crime. If biometrics data were embedded in the documents these two used; these individuals would not have been permitted to board the plane on that day. Other crimes committed through identity fraud are presented in Table 6.

Table 6

Crimes Committed Utilizing Identity Fraud

Application	Bankruptcy	Cellular
Charity	Check	Commercial loan
Computer	Confidence/Con games	Consumer loan
Credit card	Drug trafficking	Election
Food stamps	Gaming	Insurance/FALSE claims
Investors	Merchants	Medical–Health
Money laundering	Pyramid schemes	Real estate–mortgage
Securities	Social security benefits	Student loan
Telemarketing	Terrorism	Workers' compensation

Note. From "Identity Fraud: Providing A Solution," by N. A. Wilcox, Jr., and T. M. Regan, 2002, *Journal of Economic Crime Management, 1*(1), p. 17.

Consequences of IDF. A February 2009 US '08 identity fraud up in dollars survey report published by Javelin Strategy and Research showed that identity fraud victims increased to 9.9 million adults in the United States in 2008 (James Van Dyke, 2009). The reported cost was $48 billion.

Another disturbing finding of the survey was that women were 26% more likely to be victims of identity fraud than men (James Van Dyke, 2009). There were 4,800 participants in this study. In 2005, Unisys (2005) conducted a study in eight countries:

Australia, Brazil, France, Germany, Hong Kong, Mexico, the United Kingdom, and the United States. The study involved 8,339 men and women ages 18 and up. It centered on customer attitudes and awareness of bank-card fraud and identity theft as well as other fraudulent techniques and emerging anti-fraud technologies. The findings of the worldwide survey showed that:

> *Two-thirds (66%) of banking consumers worldwide worry about identity fraud and the safety of their bank and credit card accounts.*
>
> *Almost half (45%) of bank account holders worldwide are willing to switch banks for better protections from identity fraud.*
>
> *More than one-third of worldwide consumers are willing to pay additional bank fees for better security protection.*
>
> *The U.S leads in ID fraud instances (17% of U.S. consumers cite they have been victims) followed by the U.K. (11%), Brazil (9%), Mexico (8%), France (8%), Australia (7%), Germany (3%) and Hong Kong (1%).*
>
> *More Latin Americans (78% in Mexico and 70% in Brazil) worry "a lot" about the fraudulent use of their bank accounts or credit cards, compared to 23% of those in the United States. More people in Germany (17%) worry than in France or the United Kingdom (both 9%).*
>
> *Loss of money is the leading concern associated with ID fraud (27%), but also ranking high were the time and effort to fix the problem (16%, with 25% in the U.S.) and the risk of crime committed in one's name (17%, with 34% in the U.K.).*

> *Biometrics (e.g., iris or fingerprint scans) is the preferred method cited by consumers to fight fraud and identity theft, followed by smart cards, tokens, and more passwords.* (Unisys, 2005, p. 6)

In 2006, Unisys (2006) conducted a subsequent survey that randomly selected consumers from 14 countries—Australia, Argentina, Brazil, Canada, Denmark, France, Germany, Japan, Korea, Mexico, Taiwan, Thailand, the United Kingdom, and the United States. Overwhelmingly, 70% of worldwide consumers supported using biometrics technologies such as fingerprint and voice recognition to verify an individual's identity (Unisys, 2006). "This research is revealing since many headlines today seem to question adoption because of legitimate privacy concerns" (Unisys, 2006, p. 1) stated Terry Hartmann the Director for Homeland Security and Secure Identification and Biometrics. The system is very important as a common denominator in most identity deception–prone transactions.

Review of Research Methodologies

The nature of research problem will influence the selection of methodology (Leedy & Ormrod, 2001; Singelton & Straits, 2005). This study involved the increase of identity fraud in Nigeria and the investigation of dynamics that will affect the adoption of biometrics technology for recognition and confirmation of personal identity. Previous similar studies used quantitative, qualitative, and mixed method approaches. Example of such study based on quantitative method was (Brydie, 2008). Westin (2002) employed qualitative and (AlBawi, 2004) used mixed methodology.

This mixed method study started with a framework depicted in Figure 6. On the basis of this framework, four research questions guided this study. Through literature reviews, the dependent and independent variables were identified. Samples were drawn from the target population. The data from the samples were collected and statistical analyses conducted. There were various instruments of integrated methods available to investigators. The present study utilized survey and interview instruments to conduct the inquiry.

The Mixed-Method Approach and Differing Methodologies

A review of the academic and professional literature showed that the integrated method has been used in prior research to gain a better understanding of biometrics technology for identification and authentication. Scholars from diverse discipline recommended the use of mix method in a study (Garcia & Pardo, 2006) though the approach has become an issue of debate in academia. While there are several methods that can be used for scholarly inquiry, AlBawi (2004) used mixed methodology. There are exceptions to the use of integrated method as well. Such exceptions are (Brydie, 2008; Joshua & Koshy, 2009; Ngugi, 2005) who used quantitative approach and (Westin, 2002; Lease, 2005) employed qualitative technique.

Both quantitative and qualitative methods have been used extensively in studies (Onwuegbuzie & Collins, 2007). However, mixed methodology is increasingly applied in scholarly inquiry (Garcia & Pardo, 2006; Onwuegbuzie & Collins, 2007). The integrated approach has "the potential to promote the participation of multiple disciplines by

creating opportunities for multiple analyses about the same collected data" (Garcia & Pardo, 2006, p. 1). The results of the examination helped to answer the research questions.

For this study however, the survey and interview instruments were designed to focus on the dynamics that will influence adoption of biometrics security technique. The nature of this inquiry was to investigate issues of importance that affected the adoption of biometrics technology to control identity deception; and that made the selection of this approach the logical choice.

Summary

Biometrics technology promised to be a useful alternative in light of the weaknesses of the knowledge- and token-based authentication techniques currently used for identification and verification. Given the increasing threat of identity fraud and cyber-crimes as well as the global war on terror (GWOT), it is almost impossible to undermine the capabilities of biometrics technologies such as the fingerprint technique, iris scan, and face recognition. The review of the literature showed growing and favorable user attitudes toward the application of biometrics technology and the factors that influenced acceptance. The review, however, noted problems associated with biometrics technique, the intensifying criticisms, and privacy concerns.

Numerous studies have been conducted in developed countries to gain a better understanding of user perceptions of biometrics techniques and factors that affected adoption. The reports presented in this chapter increased the knowledge about causes for

biometrics adoption and as well as peoples' attitudes and behaviors toward its use for recognition, watch-listing, and confirmation of identity. Except the investigation conducted in South Africa, there was no other study that was carried out in less developed countries (LDCs) such as Nigeria. This present study addressed this gap in the literature and explored the factors that will influence the adoption of biometrics systems, with respect to awareness and the three constructs of the technology acceptance model (TAM): perceived ease of use, perceived usefulness, and security. The TAM is the theoretical framework of this study.

Understanding how to establish trust in biometrics system provides added value to preventing authentication deception. This literature review showed that acceptance of biometrics technology depended on, among other factors, providing reliable confirmation for identity management and crime control. This is significant in the context of global e-commerce, e.g., for identifying online shoppers, identity fraud, cyber-crimes, GWOT, and in the increasingly threat of illegal immigration. In chapter 3, the research methodology for the study is explained. The researcher also provides justification for the selected approach. In addition, the next chapter highlights data collection instruments, procedures, formats for results presentations, test instruments, and methods for statistical analyses.

Chapter 3: Research Method

Introduction

The purpose of this study was to investigate whether perceived ease of use, usefulness, security, and awareness of biometrics technology would influence the perceptions and behaviors of adults toward its adoption within Surulere, Lagos, Nigeria. Chapter 1 introduced the study and the problem statement, and chapter 2 presented the relevant literature on biometrics technology, identity fraud, and the technology acceptance model (TAM) that created the theoretical foundation of this study. Chapter 3 explains the research approach that was used for this mixed methodology investigation.

In this chapter, the researcher starts with a brief discussion of the reason for the chosen methodology. Next, the author presents the research design, target population, sampling procedures, sample size, instrumentation, methods for validation and reliability, data collection, and analysis. In addition, the researcher discusses descriptive, inferential statistics, plans for dissemination of research findings, and the measures taken to protect research participants. There were several research methods available to the researcher such as the qualitative approach (Creswell, 1998; Leedy & Ormrod, 2001; Silverman, 2006), the quantitative technique (Creswell, 2003; Leedy & Ormrod, 2001; Maxim, 1999), and mixed methodology (Collins & Onwuegbuzie, 2007; Creswell, 2003; Garcia & Pardo, 2006; Tashakkori & Teddlie, 1998; White, 2007).

Appropriateness of Research Methodology

The nature of the study influenced the type of methodology. AlBalawi (2004) used mixed method and concluded that there were privacy concerns in the application of biometrics as an identification approach in online courses. Brydie (2008) employed quantitative method and determined that proxemic sensitivity influenced an individual's perceived invasiveness toward hand-based biometric technologies. The research approach chosen for this study was mixed methodology, which combines qualitative and quantitative methods (Collins & Onwuegbuzie, 2007; Johnson & Onwuegbuzie, 2004; Tashakkori & Teddlie, 1998; White, 2007).

Two important justifications for the selection and application of this approach were that it increased data reliability and ensured a more comprehensive exploration of an issue or problem than would be possible in using a single method. A multi-method approach helped in obtaining better answers and increased the robustness of phenomenal understanding. According to Buber, Gadner, and Richards (2004), "mixed methods research has regained not just acceptability, but popularity, with a significant number of studies arguing its virtues in terms of greater understanding and/or validation of results" (p. 2). Johnson and Onwuegbuzie (2004) have also argued that a mixed methodology "provide[s] stronger evidence for a conclusion through convergence and corroboration of findings" (p. 21). The application of a mixed research technique in this study provided answers to a broader set of questions regarding what the reasons for acceptance were, why people were interested, what the factors that influenced adoption were, and how to use the system to control identity fraud.

In addition, a mixed methodology provided a way for this researcher to expand the scope of the study and consider other aspects of the phenomenon. Integrated methodology raised the concerns of cost for time and other resources (Garcia & Pardo, 2006; Johnson, 2006 ;Johnson & Onwuegbuzie, 2004) and challenges in sampling for combining both qualitative and quantitative methods (Collins & Onwuegbuzie, 2007). In the next section, the research design and approach is discussed.

Research Design and Approach

The research design characterized the approach for this study (Creswell, 2003) and detailed the overall process of a qualitative or quantitative study or the combination of both. Singleton and Straits (2005) stated that "to formulate a research design is to anticipate the entire research process, from beginning to end" (p. 69). Onwuegbuzie and Leech (2006) presented a framework that showed the process of using a mixed methodology or integrated approach (Figure 6). In the figure, the authors suggested a series of steps in a mixed methodology study.

These measures provided this researcher with a better understanding of the rigors of a mixed method approach and helped in the execution of the study. This mixed method study aimed to understand the factors that are barriers toward the adoption of biometrics technology for use in reliably recognizing and confirming individuals to control identity fraud. The study was descriptive, which involved the description of human-made phenomena (Gall, Gall, & Bong, 2003; Wong, Rubasinghe, & Steele, 2005).

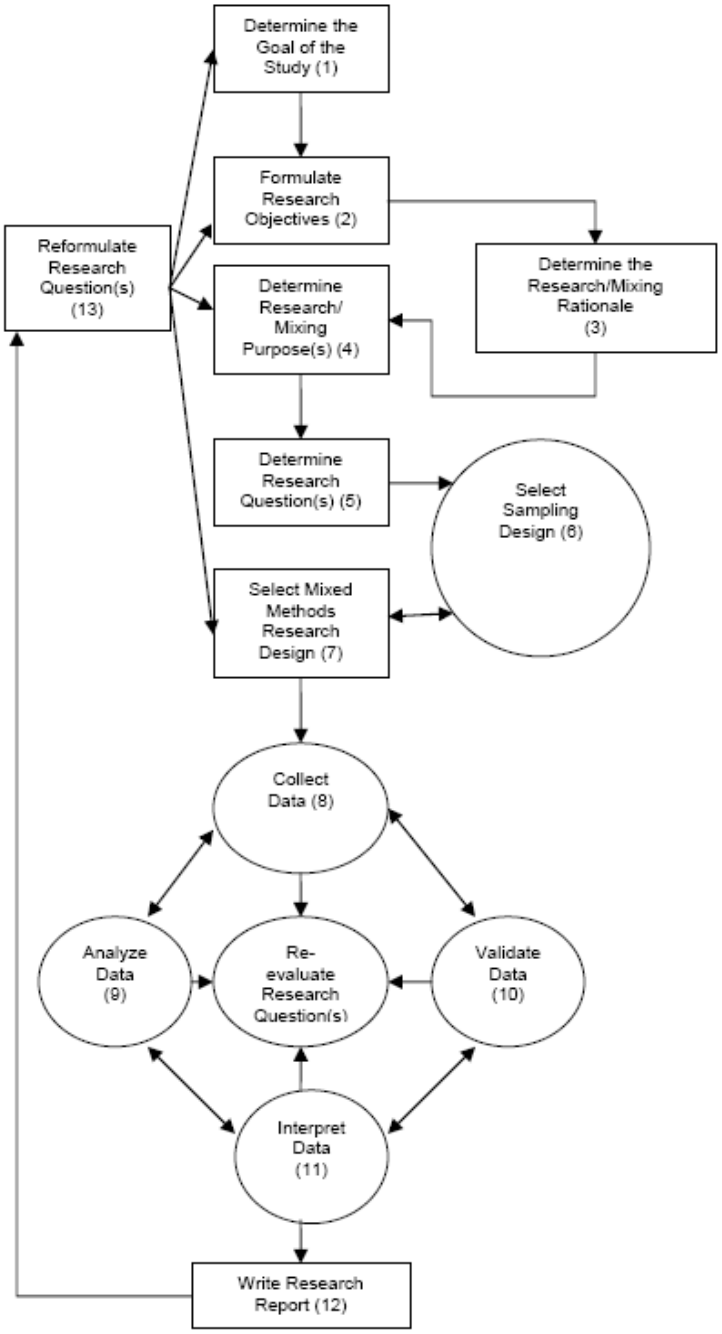


Figure 6. Steps in the Mixed Methods Research Process. From "Linking Research Questions to Mixed Methods Data Analysis Procedures," by A. J. Onwuegbuzie and N. L. Leech, September 2006, The Qualitative Report, 11(3), p. 476.

The research design and approach provided important advantages since this type of social research considered the entities to be studied, the characteristics of the entities and associated interest, and the types of relationships expected from the characteristics (Singleton & Straits, 2005). In order to state the problem in researchable expressions, the plan and method of execution influenced this research process. Given the design and approach, a set of philosophical assumptions (Creswell, 1998) were used. In this mixed methodology study, the researcher employed strategies of data collection either simultaneously or sequentially to understand the research problems (Creswell, 2003) that were addressed.

Studies conducted in Europe and the United States showed interest in biometrics technology as a legitimate form of identity authentication (LogicaCMG, 2006) despite privacy concerns (AlBalawi 2004; Crowley, 2006). AlBawi (2004) used mixed method while Westin (2002) employed the survey technique. The study by Westin compared and determined significant differences between adults' perceptions in advanced countries of those factors that affected biometrics technology adoption.

The quantitative component of this study was a survey/questionnaire used to gather demographic and awareness data. Leedy and Ormrod (2001) noted that "the approach that looks most closely at phenomena of the moment is the survey" (p. 196). Surveys are commonplace in scholarly investigations (Leedy & Ormrod, 2001). Wong, Rubasinghe, and Steele (2005) stated the advantages of the survey instrument, which were listed in Table 7.

The qualitative method employed one-on-one, semi-structured interviews. Both the survey (quantitative) and interview (qualitative) are discussed as research instruments.

During the interview, the researcher asked questions of the participants. The information/data gathered from the survey and interview provided adults' perceptions of the factors that influenced the adoption of biometrics technology. This was very useful to determine the underlying causes that affected the implementation of a biometrics system. The interview procedure is further explained in the instrumentation section. The independent variables used in this mixed method approach were ease of use, usefulness, security, and awareness of biometrics technology, and the dependent variable was adoption of biometrics and use (see Figure 7). These were discussed in Chapter 2, the literature review.

Variables: Independent and Dependent Variables

Variables

In a study, variables influence the outcome and findings. The researcher may decide on more than one variable during the investigation. For instance, a variable can take different values according to the scenario, treatment, and other issues. Investigators usually refer to variable as either independent variable (IV) or dependent variable (DV) as shown in Figure 7. While independent variable (IV) was known as believed causes, the dependent variable (DV) was regarded as the assumed outcome.

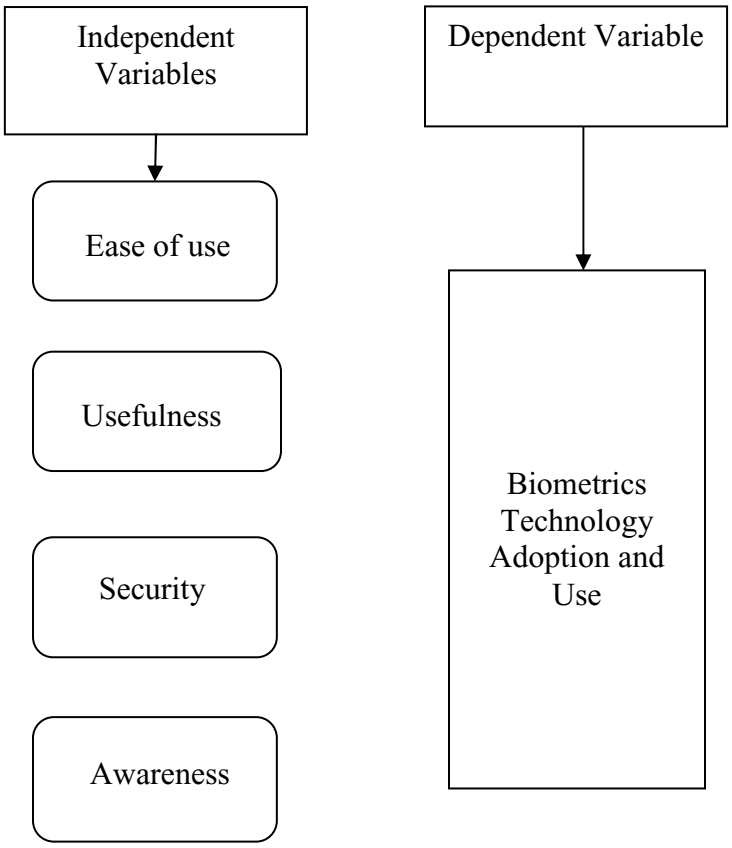


Figure 7. A graphic representation showing independent variables and the dependent variable.

Independent variables (IVs). The researcher carried out this study to determine the relationship between independent and dependent variables. The quantitative component of this investigation was appropriate because it was used to establish the relationship among independent and dependent variables. The investigator was able to interpret the study results from statistical approaches to measure the movement between the two variables. Usually, the researcher will manipulate the independent variables (IVs) for the effects on dependent variables (DVs). The independent variables used in this study are ease of use, perceived usefulness, security, and awareness.

Dependent variables (DVs). As the name suggested, dependent variables (DVs) depended on the independent variables (IVs). Usually, the investigator will develop interest in the DVs because of the effect of IVs. To execute research successfully, the investigator must determine the DVs as well as the IVs. The interaction of both has implications on the study. While there can be several DVs, in this study, the researcher used adoption of biometrics technology and use as the dependent variables. In the next section, the researcher discusses the target population, sampling procedure, and sample size.

Target Population, Sampling Procedure, and Sample Size

Population

The basic research paradigm defined the population from which the target research subjects were selected. This gave the researcher the opportunity to conduct the study on the target population and inferred the results of the study from the sample back

to the population (Walonick, 2005) from which the sample was selected. This research aimed to understand the issues that affected the adoption of biometrics technology. In the majority of studies, it was impossible to survey the entire population (Podder, 2005). This provided the rationale to use a target population.

The target population of the study was adults who lived in Surulere, Lagos, Nigeria and who were familiar with biometrics technology such as fingerprint and iris scans. The study participants were literate. In a study, the target population represented a collection of participants of interest to the researcher (Singleton & Straits, 2005). Similarly, Maxim (1999) stated that population is "the set of all elements bounded by a particular set of time-space coordinates; for example, all people living within the geographical boundaries" (p. 107).

The participants for this study were drawn from private and public places such as banks businesses, and government offices through personal contacts. The target population of this study was 120 to 140 people for the qualitative and quantitative approach because of the research subject of biometrics technology, such as fingerprint recognition and iris scan. This sample was further explained in chapter 4, Results. This researcher did not have equal numbers of male and female as participants. However, the screening process helped the researcher determine how many of each gender took part in the study as illustrated in chapter 4, Description of Variables.

Sampling Procedure

Sampling is the method of selecting "a portion, piece, or segment that is representative of a whole" (Onwuegbuzie & Collins, 2007, p. 281). A major requirement in conducting research is the selection of a sample or a subset of the population (Leedy & Ormrod, 2001). The sample was helpful for the researcher to make quality decision that stemmed from the findings (Onwuegbuzie & Collins, 2007). This study utilized purposive sampling. This implied that there was a purpose in mind for carrying out such a study (Creswell, 2003). A purposive sampling is a method wherein one or more specific and predefined groups are the focus of the study. This allows for the purposeful selection of participants or sites that best help the researcher to understand the problem and answer the research questions (Creswell, 2003).

Since purposive sampling was used, the ability to generalize to a larger population is impossible. This is a disadvantage of this sampling strategy. Singleton and Straits (2005) stated that "purposive sampling for heterogeneity and/or typicality is unacceptable substitute for probability sampling when precise and accurate generalizations are required. However, with studies of more limited scope or in situations that preclude random selection, purposive sampling is an acceptance alternative" (p. 134). Purposive sampling is very useful for a study because it allows the target sample size to be reached quickly. The outcome of the study could then be generalized to the target population from which the participants were selected. In general, purposeful sampling provided a way to determine the views of the target population (Asfaw, 2006).

During this research, adults within Surulere, Lagos, who were literate and over 18 years of age constituted the sample of this study. They were screened for biases and determined that they were aware but not users of the technology. This helped satisfy the need of the research. In sampling "much depends on the professional and financial resources available" (Wong, Rubasinghe, & Steele, 2005, p. 13). For instance, if there was no adequate financial resource available, it was not feasible to sample the population beyond a manageable size.

Sample Size

The selection of sample size is an essential element of phenomenological investigation. Bartlett, Kotrlik, and Higgins (2001) stated that, "Sample size is one of the four inter-related features of a study design that can influence the detection of significant differences, relationships or interactions" (p.43). Sample size is critical because "it provides a basis for the estimation of sampling error" (Leedy & Ormrod, 2001, p.140). The authors warned that:

> A small sample could lead to acceptance of a model which is not necessarily a good fit, simply because there was not enough statistical power to reject the model. On the other hand, if the sample is too large, the model may be rejected due to sensitivity in detecting small differences, because the larger the sample, the more sensitive the test is to detecting differences (p. 140).

In this study, adults in Surulere, Lagos, who were literate and over 18 years of age and were knowledgeable about biometrics were participants. The responses collected

were an approximate representation of the target population. Maxim (1999) stated that "sample is a subset of a population chosen according to some procedure that allows for the observation and measurement of elements fewer than the population" (p. 107). The sampling of the target population provided the number of participants who took part in the study. The following questions were asked to screen and qualify research subjects:

1) Are you willing to take part in this study?
2) Are you over 18 years of age?
3) Can you read and understand the English language?
4) Are you familiar with biometrics technology?
5) Do you know about fingerprint and iris scan?

As already stated, 100 to 140 subjects were the sample size of this study. This was determined from those who answered yes to the above questions. These individuals were then invited to participate in the study. Although there were applications such as sample size calculator (Creative Research Systems, 2009) used to determine sample size, the 100 to 140 study subjects were justified due to the topic biometrics technology such as fingerprint and iris scan.

Dominic (2007) stated "that obtaining the appropriate sample size is very important. Too large a sample may waste time, money, and resources; but too small a sample may lead to inaccurate results" (pp. 53–54). Budget, time, and personnel were various constraints that faced the researcher, which affected sample size (Bartlett, Kotrlik, & Higgins, 2001). Further justifications of the sample size were: the study was

conducted overseas, the constraints of financial resources, logistical impediments, unreliable communication infrastructures, and the level of awareness of the technology. Podder (2005) stressed the importance of a small sample size of a target population and noted that it can yield high accurate predictions if the subjects were selected properly.

To conduct the study, participants were assigned unique codes, which provided confidentiality. Such codes were determined during data collection and analyses. The method of coding ensured that they remained anonymous to each other and to the reader. In this way, the confidentiality and anonymity of the subjects were addressed and maintained (Creswell, 1998). The informed consent, confidentiality, location, and study instruments are discussed in the next section.

Informed Consent, Confidentiality, Location, Instrumentation, Survey, Interview, and Pretests

Informed Consent

The Belmont principle required human subjects that participated in research to provide voluntary consent (Cassell, 2000). In voluntariness, the researcher must not influence or coerced the participant. In the process, the participant had the mental ability to assess and comprehend the information presented in the research instrument in order to make an informed decision. The researcher was also required to disclose useful information to the participant such as the purpose of the study, any associated risk, potential benefits, and contact information (Cassell, 2000).

Each study participant was informed that participation was voluntary and given the informed consent form to complete (see Appendix B). Every adult participant

reviewed and signed the form before taking part in the study. If a member of the study group chose not to complete the informed consent form, the subject did not participate. The importance of the informed consent form proved that research subjects were not unduly influenced or forced to take part against their will. Moreover, people were reminded that anybody can withdraw from the study if the person wished to do so. The issue of confidentiality is discussed next.

Confidentiality

The need to uphold the confidentiality of personal information is very important when human beings participate in research. This ensures willingness, cooperation, and honesty in the interviews and in response to the Likert-type survey questions. Every participant was given the opportunity to read the confidentiality agreement and then sign it (see Appendix C). Creswell (1998) emphasized the importance of confidentiality in conducting a study. Providing a statement of confidentiality to participants fosters a sense of trust, which in turn influences survey response rate (Podder, 2005) and cooperation during the interview. The confidentiality of research participants' data was protected to avoid accidental disclosure or other forms of breach and compromise. De-identifying personal data through coding and anonymizing helped to protect participants' confidentiality. This ensured their cooperation in this study. The location of the study is discussed next.

Geographic Location

This study was not conducted through an electronic survey. As a result, the location was very essential both to meet the participants and also conduct the study. The target population for this investigation was selected from adults living in Surulere, a business district in Lagos, Nigeria. The sample was confined to adult Nigerian citizens because of the nature and importance of the study. Surulere is an ideal environment for this study as a district, and Lagos, as a city, being a major financial, commercial, and industrial center. Lagos was categorized as one of the top megacities of the world and it was expected that the business districts around will experience similar population growth. Each participant selected for this research was contacted for the purpose of conducting one-on-one, semi-structured interviews and to administer the Likert-type questionnaire (Slover, 2007). The study instrumentation is discussed next.

Instrumentation

For this study, instrumentation was part of the rigor for data collection (Creswell, 2003). There were two distinctive tools used for this study, survey questionnaire and interview. The survey was designed to incorporate demographical and awareness of biometrics attributes to obtain response that suited the need of the investigation. The interview was the direct interaction between the investigator and the study participants. Usually, it required social skills and fast thinking (Podder, 2005). For the survey, the items of the questionnaire were reviewed by the chairperson, Dr. Raghu Korrapati, for

content validity. The recommended changes were incorporated into the survey instrument. The researcher discusses these instruments in more detail below.

Survey as quantitative instrument. Survey is the common method of data collection in research (Singleton & Straits, 2005). There are two types of survey questions, open-ended and closed-ended inquiries. Open-ended (free-response) questions permit the participants to express response; closed-ended (fixed-choice) questions only allow for the selection of answers from available options (Singleton & Straits, 2005). The researcher used the closed-ended survey method for this study.

The survey provided flexibility to participants of the study because their time was not constrained, compared to an interview. The incidence of nervousness was also eliminated, which posed a limitation in answering interview questions. Surveys, when standardized for all respondents, tended to enhance reliability of data (Singleton & Straits, 2005). See Table 7 for an enumeration by Wong, Rubasingle, and Steele (2005) of the benefits of the survey technique of data collection.

Appendices A and B contain the survey cover letter and the consent statement for this study, respectively. Appendix D presents the survey instrument. It was divided into five sections. The first segment contained multiple choice questions related to demographical and awareness attributes. Responses of “Yes” or “No” were answer options. These items were intended to uncover the usefulness, ease of use, security, awareness, attitudes, behaviors, opinions, and other issues that impacted the adoption of

biometrics technology. Sections 2, 3, and 4 were presented on a 5-point Likert-type rating scale.

The scale consisted of a series of declarative statements. Response selections were: *Strongly Agree, Agree, No Comment, Disagree, and strongly Disagree*. The participants were required to show if they strongly agree, agree, had no comment, disagree, or strongly disagree with each statement. The corresponding numbers to each possible selection allowed quantification of the responses, which were summed across survey items and arrived at a total score for each participant. The scale was further discussed in the data analysis section. The Likert-scale and statistical tests were used to measure the items on the survey instrument. The next instrumentation that the researcher discusses is the interview.

Table 7

Advantages and Disadvantages of the Survey Research Method

Advantages	Disadvantages
Surveys are relatively inexpensive	
Useful in describing the characteristics of a large population. No other method of observation can provide this general capability.	A methodology relying on standardization forces the researcher to develop questions general enough to be minimally appropriate for all respondents, possibly missing what is most appropriate to many respondents.
Can be administered from remote locations using mail, email, or telephone.	Inflexible in that they require the initial study design (the tool and administration of the tool) to remain unchanged throughout the data collection.
Very large samples are feasible, making the results statistically significant even when analyzing multiple variables.	The researcher must ensure that a large number of the selected sample will reply.

(table continues)

Advantages	Disadvantages
Many questions can be asked about a given topic, giving considerable flexibility to the analysis. Flexibility at the creation phase in deciding how the questions will be administered: as face-to-face interviews, by telephone, as group administered written or oral survey, or by electronic means. Usually, high reliability is easy to obtain—by presenting all subjects with a standardized stimulus, observer subjectivity is greatly eliminated.	It may be hard for participants to recall information or to tell the truth about a controversial question.

Note. From "An Empirical Research Program for Biometric Technology Adoption," by Y. K. Wong, A. Rubasinghe, & R. Steele, 2005, Proceedings of *IRIS: 28 Conference*, Kristiansand, Norway, August 6–9, p. 13.

Face-to-face interview as qualitative instrument. One of the methods used in research is the face-to-face interview. It is a major source of useful information during the investigation (Silverman, 2006). An interview is a direct meeting and interaction between the interviewer and interviewee. A standardized interview instrument follows the same pattern, where questions are asked of the respondents and the interviewer later codes the participants' answers (Cano, 2009) using suitable techniques and software.

During the interview, "the primary concern is maximizing the flow of valid, reliable information while minimizing distortions of what the respondent knows" (Silverman, 2006, p. 141). The interactional nature of interviewing makes it unique. However, "the need to keep that interaction in check" (Silverman, 2006, p. 141) is important in order not to taint the interview result. To conduct face-to-face interviews for this study, the target population was purposefully selected from the population, as the

researcher discussed earlier. An interview protocol (see Appendix E) was administered to the participants to ensure successful interview sessions. The protocol was a prepared, structured document that guided the interview process (Dominic, 2007). The interview protocol was:

> a predetermined sheet on which one logs information learned during the observation or interview. Interview protocols enable a person to take notes during the interview about the response of the interviewee. They also help a researcher organize thoughts on items such as headings, information about starting the interview, concluding ideas, information on ending the interview, and thanking the respondent. (Dominic, 2007, pp. 60–61)

The research subjects were asked to explain in their own words, thoughts, feelings, attitudes (Slover, 2007), and factors that would influence the implementation of biometrics technology. The interview protocol and writing notes were used for data collection. The questions that were asked the participants were contained in the protocol (Appendix E), which provided a guide for how the interview proceeded. In order to guarantee a successful interview, the study incorporated the recommendations of (Creswell, 1998):

1. Locating site or individual
2. Gaining access and making rapport
3. Collecting data
4. Recording information

5. Storing data. (p. 110)

Each session of the interview lasted between 30 to 45 minutes. This was necessary so that participants did not get bored. The researcher established and maintained rapport with the interviewees. At the end of the interview, there was time for further comments that encouraged constructive feedback. In the next section, the researcher discussed pretest, validity, and reliability.

Pretest. After the Institutional Review Board (IRB) of Walden University granted approval 05-04-10-0209264 on 4 May 2010 of the proposal to conduct research, a pretest was conducted. Pretesting is the final stage in the questionnaire development process where the research instrument is administered in a small pilot study and the researcher determines if the questionnaire will work well (Hunt, Sparkman, & Wilcox, (1982). The purpose is to ascertain the appropriateness of research questions relative to participants' knowledge (Leedy & Ormrod, 2001; Singleton & Straits, 2005). It is a critical step (Blair, 2010) and is considered a dry run, where defects in the questions are discovered (Narins, 1999). As Hunt, Sparkman, and Wilcox, (1982) pointed out, "no amount of intellectual exercise can substitute for testing an instrument designed to communicate with ordinary people" (p. 269). This was important to obtain valuable feedback from pretest participants and make corrections to the research instrument.

In pretesting, Hunt, Sparkman, and Wilcox (1982) pointed out that five fundamental issues should be resolved and they are: (1) What specific items should be pretested? (2) What method should be used to conduct the pretest? (3) Who should do the

pretesting? (4) Who should be the subjects in the pretest? (5) How large a sample is needed for the pretest? (p. 269). The answers to these questions help determine if the research participants understood the questions (Creative Research System, 2009). In addition, the researcher is also better prepared to update the research instrument where appropriate.

There are several methods available for pretesting research questionnaires: conventional pretests, behavior coding, and cognitive interviewing (Blair, 2010; Presser & Blair, 1994; DeMaio, Rothgeb, & Hess, 1998). Other techniques are expert panels, questionnaire appraisal coding systems, and interviewer debriefings (DeMaio, Rothgeb, & Hess, 1998) focus group, and field testing (Blair, 2010).

Whereas cognitive interviewing identifies problems that cause difficulty for the participant, a conventional pretest seems to be effective for identifying issues that cause difficulty for the interviewer. The behavior coding was helpful and diagnosed uncertainty about attribute to questions (Presser & Blair, 1994). These approaches are significant in that they affect the ability of the questionnaires to function as intended. In this study, expert panel and questionnaire appraisal were used.

The pretest was conducted among Nigerians who resided in the Washington, D.C., metro area. The purpose of the pretest was to determine the reliability of the research instrument. The relationship between the pretest participants and the larger study group was to determine the suitability or feasibility of the research instrument. It also provided an indication of sample size for the study. There were ten immigrants from

Nigeria that participated in the pretest. The entire survey procedure lasted approximately 30 minutes and followed receipt of consent to participate from each respondent.

The researcher instructed the participants not to discuss the pretest for control of opinion diffusion. The candidates that participated for the pretest provided feedback on the research tool. The pretest participants' suggestions were incorporated into the study instrument that decreased the chance of losing valuable respondents. The significance of validity and reliability in research execution is presented next.

Validity and Reliability

Validity

The issue of validity is central to and seen as strength in social research (Creswell, 2003; Silverman, 2006). Usually, validity addresses whether the operational indicators are true (Maxim, 1999). Validating research instruments is necessary since the objectivity of the study can be questioned (Silverman, 2006). According to Joppe (2000):

> Validity determines whether the research truly measures that which it was intended to measure or how truthful the research results are. In other words, does the research instrument allow you to hit "the bull's eye" of your research object? Researchers generally determine validity by asking a series of questions, and will often look for the answers in the research of others. (p. 1)

The validation of survey instruments is critical for avoiding deficiencies in how questions are framed. If questions are not asked correctly, this may lead to responses that are inaccurate. Shanks, Tansley, and Weber (2003) stated that the accuracy of the

instrument depends on (a) accuracy of the instrument, (b) completeness to represent the goal of the study, (c) conflict-free to avoid contradiction, (d) non-redundant to avoid conflict if and when the instrument is updated (p. 86).

One of the methods of validation is to engage expert opinion regarding the relevance of the instrument before it is administered to the participants. To validate the survey tool, experts like Dr. Raghu Korrapati were engaged on the basis of his teaching experience and several years of research skills in chairing doctoral students through the dissertation process. In addition, members of the dissertation committee and other colleagues from the field of information systems management reviewed the instruments and assessed content validity. The feedback from conducting the pretest also provided input for research instrument validation.

Maxim (1999) stated that, "content validity reflects subjective judgment about whether an indicator references that which it is supposed to reference" (p. 208). Reviews by these experts provided constructive feedback that eliminated deficiencies and confirmation that the designed instrument was suitable for data collection. The content validity and content-related evidence were verified when the pretest was administered. Therefore, this proved the validity of the research instruments.

Reliability

Reliability is very important so that no accidental circumstances of the research (Silverman, 2006) affect the result. If a measuring tool yielded a certain result when the entity measured has not changed, then the study results were reliable (Leedy & Ormrod,

2001). Reliability measure is an empirical attempt to understand the truth in relation to natural phenomenon (Woods, 2009). The main elements of reliability in research tool are accuracy and consistency (Leedy & Ormrod, 2001).

The study instruments were administered precisely and dependably to the study participants. The researcher also considered the concerns of research participants when the research tools were developed. The pilot study conducted provided measure of reliability because the participants understood the statements in the research instrument used. The feedback that the participants provided helped the researcher to clarify the research questions and statements. In the next section, the researcher discusses data collection, data analysis, descriptive statistics, and inferential statistics.

Data Collection, Data Analysis, Descriptive Statistics, and Inferential Statistics

Data Collection

As stated earlier, after the Institutional Review Board (IRB) of Walden University granted approval 05-04-10-0209264 on 4 May 2010 of the proposal to conduct research, data collection was necessary. Creswell (1998) stated that "data collection offers one more instance for assessing research design within each tradition of inquiry" (p. 109). During the study, data collection was very important as a means for the preparation and measurement of variables that interested the researcher.

Creswell (1998) documented the process of data collection activities such as (a) locating site/individual, (b) gaining access and making rapport, (c) purposefully sampling, (e) collecting data, (f) recording information, (g) resolving field issues, and (h)

storing data (p. 110). Similarly, the type of data, location, security, and interpretation (Leedy & Ormrod, 2001, p. 111) affects collection. The methods selected for data collection were a survey administered to the participants and structured interviews, which were conducted in person. These approaches helped the researcher to generate data and understand the problems addressed in this study.

As noted earlier and defined, purposive sampling was employed for the selection of research subjects. The interview, as an instrument that allows for active participation, has already been discussed. Creswell (2003) explained the advantages of interviews since: (i) participants can provide historical information, and (ii) allows the researcher "control" over the line of questioning (p. 186). Prodder (2005) suggested that interviews provide the opportunity for every respondent to participate.

The investigator can make more valid interpretations, and there is direct contact with research participants. Surveys through questionnaires (Leedy & Ormrod, 2001; Maxim, 1999; Singleton & Straits, 2005) and structured face-to-face interviews (Creswell, 2003; Dominic, 2007; Slover, 2007; Leedy & Ormrod, 2001) were instruments used to collect data from participants. The data collected were analyzed using statistical packages, tools, and software. The results are presented in chapter 4. In the next section, data analysis is presented.

Data Analysis

In qualitative and quantitative research, otherwise known as mixed methodology, data usually are integrated during analysis to transform one data type to another

(Caracelli & Greene, 1993). During this study, there were various methods available for data analysis such as statistical package for the social sciences (SPSS), statistical analysis system (SAS), Microsoft Excel application, and Nvivo software. The data collected for this study were analyzed, which determined the outcome of the investigation (O' Connor, 2006).

Data "must be manipulated further so that their meaning and bearing on the problems and hypotheses that initiated the inquiry can be extracted" (Singleton & Straits, 2005, p. 71). In mixed methodology research, data analysis involves the description of information through the techniques selected (Creswell, 2003). Data were analyzed from survey findings and interviews to produce more robust outcomes. The result of the analysis presented in chapter 4 answers the research questions of the factors that influence the adoption of biometrics technology.

A Microsoft Excel spreadsheet was used for coding and analyzing the Likert-scale items. This tool was appropriate since the questionnaire was divided into several segments and each addressed a research question. Rensis Likert developed the scale in 1932 (Bucci, 2003) and has since become a major research methodology tool used for measurement. The scale was particularly used as an assessment technique to measure attitude (Bucci, 2003). Likert scale provided an effective approach to obtain consistent survey responses (Parnaby, 2007).

Research participants usually made decisions on their level of agreement, generally on a five point scale such as (Strongly Agree, Agree, Disagree, No comment,

and Strongly Disagree based on a set of statements (Bucci, 2003; Parnaby, 2007). Likert scale was justifiable to be used in this research for data measurement because it was relatively easy to construct, yielded highly reliable scores, flexibility to measure different characteristics, and easy to read and complete (Bucci, 2003). The drawbacks however, were the difficulty to demonstrate validity and absence of one-dimensionality and homogeneity.

The researcher did not analyze data using Chi-square. Chi-square is used when both dependent and independent variables are categorical. The only categorical variables in the analysis were gender and adopt biometric technology (yes or no). The other variables were continuous and not applicable for the Chi-square analysis. NVivo version 7 software was used to categorized and identified key words and phrases from the interview data.

This is presented in the qualitative component of this study in chapter 4. The Excel spreadsheet and the statistical package for the social sciences (SPSS) version 18 were used for data analysis. The researcher coded information into the Excel spreadsheet and later imported the raw data into SPSS and conducted further statistical analysis. The nature of the data analysis was descriptive. The results are also presented in chapter 4. In the next section, the researcher discusses descriptive statistics.

Descriptive Statistics

For this study, the researcher used both descriptive and inferential statistics. Descriptive statistics are very important for data interpretation. They are used to describe

coefficients about a given data set, which can either be a representation of the entire population or a sample (Investopedia, 2010). Within data, there are different variables that can be correlated with one another (Leedy & Ormond, 2001). Such correlation can be used to understand data that was collected from a study. The measures used to describe the data set are measures of central tendency or mid point and variability or dispersion (Leedy & Ormond, 2001).

With descriptive statistics, the researcher or the investigator simply describes what is or what the data show (Trochim, 2008). There are several measures and descriptive statistics are used to present quantitative descriptions in a manageable form (Trochim, 2008). In other words, descriptive statistics reduce data to simplified summary. Such data can be presented in bar charts, pie charts, and histograms for visualization, understanding, and interpretation. There may be either lots of measures or large number of people on any measure during a study. However, descriptive statistics helped the investigator to simplify large amounts of data in a sensible way. Each descriptive statistic reduced lots of data into a simpler summary for interpretation. Another form of statistics is known as inferential statistics

Inferential Statistics

This form of statistics allows a researcher to make conclusions or inferences about large populations through collection of data on relatively small samples (Leedy & Ormond, 2001). A small population can be used to estimate the characteristics of the larger population. More importantly, inferential statistics provide the mechanism for the

researcher to make reasonable guesses about a large, unknown population through a small sample that is known (Leedy & Ormond, 2001). Most of the major inferential statistics include the General Linear Model and analysis of variance (ANOVA), the *t* test, regression analysis, analysis of Covariance (ANCOVA), and factor analysis (Trochim, 2006).

After analyzing the data collected from administered questionnaires and interviews, the dissemination of the result of the study is very important. There were several measures for the propagation of the research findings. In the next discussion, the researcher describes plans necessary for dissemination of the research results and how the privacy of research participants was and will continue to be protected.

Dissemination of Research Findings and Protection of Research Participants

Dissemination of Research Findings

The dissemination of study findings is very important and in most times, researchers neglect to incorporate this aspect of the investigation into the research plan. The dissemination of research results ensures that members of the public, academia, industries, the media, and other interested parties understand the importance of controlling identity deception and the role of biometrics technology in that regard. To disseminate the findings of this study, the researcher will develop a strategy that will incorporate the recommendations of the International Development Research Center (IDRC, 2011).

One of the measures the researcher will use to disseminate the study findings is through collaboration. The researcher will team up with Dr. Raghu Korrapati, who is the Editor-in-Chief of the International Journal of Applied Management and Technology (IJAMT) and also the chairperson of this research, to publish an article about the results of this study. The IJAMT is a peer-reviewed journal of Walden University and has wide readership and circulation in the fields of applied management and applied technology.

Other plans that the researcher will implement for the dissemination of the findings will include making contact with the embassies of African governments in Washington, D.C., and provide documentation of the research to generate interest at that level. The researcher also plans to write press releases, use Internet listervs on special topics that relate to the research, multimedia slides, conference presentations, seminars, presentations as a guest speaker at events, articles in community or ethnic newsletters, workshops, linking the study results to other articles of importance (IDRC, 2011), and distribution of the research findings to major stakeholders in the biometrics industry. Next is the discussion of how to protect the rights and welfare of research participants.

Protection of Research Participants

The use of humans in research has raised the issue of participants' data protection and privacy. After Walden University's Institutional Review Board (IRB) granted written approval to conduct this study, the researcher completed training about the involvement of humans and the research implications. The National Institute of Health (NIH) conducted this course. The researcher completed the training and obtained a Certification

Number 355730 dated January 6, 2010 (see Appendix I). The purpose of the course was to provide useful information about the researcher's responsibilities to protect the privacy and identity as well as the rights and welfare of the research participants.

Based on the purpose of protecting research participants' privacy and confidentiality, the researcher will:

- Not disclose participants' data to third part vendors without written permission of the participants
- Be the only person who will maintain the database and other data storage drives and devices
- Safeguard participants' data through access control mechanism (user name and password required) to mitigate unauthorized right to use
- These measures will ensure data confidentiality, safeguard the privacy of participants, meet the objective of NIH mandate of protecting the rights and welfare of humans who participate in research

Below is the research questions mapped to the survey items.

Research Questions Mapped to Survey Items

Research Questions	Survey Items
1. What is the relationship between ease of use and user perceptions toward adoption of biometrics technology for control of identity fraud?	Sections 1 and 2 in conjunction with Appendix E.
2. What is the relationship between perceived usefulness and acceptance of biometrics technology for control of identity deception?	Sections 2, 3, 4, and 5 in conjunction with Section 1.
3. What is the relationship between security and user perception toward adoption of biometrics system for control of identity fraud?	Section 4 in conjunction with Appendix E and the literature review.
4. What is the relationship between awareness and the adoption of biometrics technology for control of identity deception?	Sections 1, 4, and Appendix E in conjunction with the literature review.

Summary

In this chapter, the researcher presented the research methodology that was used for this study. The integrated approach, or mixed method, was chosen as it was well suited to uncover peoples' perceptions and interests about the factors that influence the adoption of biometrics technology for identity management. The chapter also discussed the research design and instruments that were used with the study participants. In addition, this chapter highlighted the appropriateness of the research design, depicted the research process, and described the target population, sampling procedure, sample size,

and the advantages and disadvantages of the survey instrument, as well as validity, reliability, data collection, and analysis.

This chapter also provided plans for the dissemination of research findings and the completion of NIH training on how to protect research participants' rights and welfare. Chapter 4 discusses the analysis using statistical tools and the results in relation to the research questions. Chapter 5 presents the summary, conclusion, and recommendations for future research.

Chapter 4: Results

Introduction

The purpose of this study was to investigate the dynamics that influence the implementation of biometrics technology for the control of identity fraud within Lagos, Nigeria. This chapter presents the results of the interviews conducted and the data analyses of the survey questionnaire that was administered to adults who participated in the study. To help the reader understand this investigation, there were four research questions that guided the study:

1. What is the relationship between ease of use and adults' perceptions toward adoption of biometrics technology for control of identity fraud?

2. To what extent, if any, is biometrics technology considered a reliable mechanism for identity verification? And what is the relationship between perceived usefulness and the acceptance of biometrics technology for control of identity deception?

3. What is the relationship between security and adults' perceptions toward adoption of biometrics technology for control of identity fraud?

4. What is the relationship between adults' awareness and the adoption of biometrics technology for control of identity deception?

To answer the study questions, this chapter is organized into these sections: instrumentations, qualitative analyses for the interviews, and quantitative analyses for the survey questionnaires. In the first segment of these analyses, the author discusses the instrumentations used for this mixed methodology study.

Instrumentations

Survey cover letters and interview protocols were the instruments used for this study. The survey cover letters were used to invite participants for the study. The purpose of the survey cover letters was to inform the participants about the study and solicit information on how factors such as ease of use, usefulness, security, and awareness affect the implementation and usability of biometrics technology for reliably recognizing and confirming peoples' identity within Nigeria. The survey required adults to answer demographic questions and short response answers. Similarly, the interview protocols invited participants who were literate, of adult age, familiar about biometrics informed consent, allowing the participants to understand the study before deciding whether to take part.

The consent forms stipulated that participation was voluntary and there was no compensation for participating. Any participant was free to leave at any time. Letters and consent forms (Appendices A and B) that described the nature and importance of the study were given to potential participants. The researcher contacted potential participants through telephone calls and direct contact. One of the methods generally used is the face-to-face interview because it is a useful instrument for gathering data (Silverman, 2006). Face-to-face interviews were conducted before the survey questionnaires were distributed to the sample of the target population. During the interviews, the interview protocol (Appendix E) was given out to each interviewee. All interviews were documented and transcribed. The researcher then analyzed and interpreted the results according to the categorized that were identified.

The Interview Sample of Population and Settings

In the qualitative component of this mixed-methodology study, the researcher carefully selected 20 research subjects out of a total sample of 150. Of this number, 11 (55%) participants were male and 9 (45%) were female. The participants that were selected and interviewed were familiar with biometrics technology. The study participants consisted of bank employees, business professionals, students, and government employees. The researcher conducted the interview on a one-on-one semi-structured basis within the respondent's own facility. This type of setting allowed the interviewees to adjust to a familiar environment. Each interview lasted between 30 and 45 minutes.

Data Collection

The data collection did not commence until after the researcher received approval to conduct research from Walden University's institutional review board (IRB). The IRB approval for this study was 05-04-10-0209264, granted on 4 May 2010. The data collection process for the qualitative component consisted of conducting one-on-one, semi structured interviews. A Likert-type questionnaire was utilized for the quantitative component of this study. The mix of the qualitative portion of the investigation and the quantitative component contributed to the mixed-methodology approach (Albalawi, 2004; Asfaw, 2006, Slover, 2007) that was used for this study. The survey component of the data collection will be presented after the qualitative section. Through the use of interviews, participants' opinions regarding the factors that influence the implementation

of biometrics technology to control identity fraud in Lagos, Nigeria were explored. During the preparation of the qualitative component of the study, the researcher followed the recommendation of authors such as Slover (2007) for a step-by-step process of conducting one-on-one, semi-structured interviews as is depicted in Table 8.

Table 8

Step by Step Process for Conducting Interviews

Sequential Steps	Description
Step 1	Selected participants who were a representative sample population of the subject under investigation.
Step 2	Established a rapport with each participant at the beginning of each interview by describing the purpose of the study.
Step 3	Ensured that each participant understood the nature and purpose of the study and that a consent form was signed, indicating their agreement to participate in the study.
Step 4	Focused on the experiences, knowledge, and attitudes of the participants.
Step 5	Documented each interview as part of the data collection process.
Step 6	Used a one-on-one, semi-structured interview technique that allowed interviewees to answer research and follow-through questions that were posed to them by the researcher.
Step 7	Transcribed and documented the interviews.
Step 8	Removed the names of the participants from the transcribed data to ensure the confidentiality of data and personal information.

Note. From "A Case Study: Why Commercial Health and Fitness Facilities Achieve Defined Key Performance Indicators," By E. M. Slover, 2007, Unpublished doctoral dissertation, p. 84.

Before the interview, the investigator contacted each prospective participant through telephone calls, in-person contacts, and provided an explanation about the nature and purpose of the study. The name and contact information of research subjects who expressed interest to participate in the study were collected prior to scheduling the interviews. In August 2010, the researcher traveled to Lagos, Nigeria, and conducted the study (interviews and survey). Each session of the interview lasted between 30 to 45 minutes. Prior to the interview, the researcher informed the participants there was no compensation to be given, it was voluntary, the risk to participate was minimal, which was the time for participation and there was no benefits.

The interview participants voluntarily agreed to participate in the study and granted permission to be interviewed. The researcher provided the research subjects with the informed consent form and the confidentiality agreement that explained the purpose of the study, the protection of each participant's privacy, and their role in the investigation. The study participants signed the consent forms prior to the interview (see Appendix B). As stated earlier, each interview was conducted in the participant's own location, which allowed the respondent to express perspectives in a familiar environment.

The sample for this interview was 20 research subjects and the researcher interviewed every participant separately and privately. The sample size was small so that the investigator could ask in-depth questions of each participant. The smaller the size, the more in-depth the researcher probed for more responses. Of the 20 interview research subjects, there were 11 (55%) males and 9 (45%) females. The interview protocol

(Appendix E) was used to administer the interview. According to Creswell (1998), the instrument was organized in the following areas such as: “headings, information about starting the interview, concluding ideas, information on ending the interview, and thanking the respondents” (p. 126). Copies of the instrument were made available to interviewees ahead of the session because it helped the participants to organize their thoughts and opinions, which made the process orderly.

During the interview, each participant expressed opinions and varied experiences. It was a process for the researcher to conduct the qualitative component of the study. It provided the researcher the one-on-one, semi-structured, open-ended nature of the interviews, which allowed flexibility for dialogue with the participants and the exploration of the topic as the interview proceeded (Slover, 2007). The interview protocol (Appendix E) had four main questions and potential follow-up questions, which depended on the responses to the main questions. The interview protocol simplified the interview process through maintenance of a logical, continuous sequence of questions, and ensured consistency among the participants (Slover, 2007). The researcher structured the interviews, which encouraged participants’ feedback and gave them some flexibility to explore the factors that would influence the adoption of biometrics technology for control of identity fraud within Nigeria.

The interview instrument was a useful mechanism for data comparisons (Albalawi, 2004). During the interviews, the researcher used questions from the interview protocol (Appendix E) for evaluation and comparison of data among the participants. The

researcher collected data through the documentation of responses in a research log as well as in transcriptions of the interviews. The investigator assigned unit numbers to the participants. To achieve validity, the researcher provided each participant with a copy of the transcript and requested feedback about the accuracy of their opinions as expressed in the interview.

Many authors (Albalawi, 2004; Asfaw, 2006; Dominic, 2007; Slover, 2007) have used interview transcription in their respective studies. The transcriptions of the interviews are essential elements of the qualitative research component, since the researcher explored the transcripts and identified and organized the elements of the responses into a logical sequence of activities (Slover, 2007). The content of the transcribed interviews was gained from documentation and field notes in the research log that ensured accuracy of the descriptions that each participant provided. Each interview consisted of providing a description of the research study, documenting the responses of adult participants, and identifying the factors that influence the implementation of biometrics technology for the control of identity fraud.

Data Analyses—Qualitative Component

The analyses of qualitative data can be achieved through emergent themes that highlight the interconnectivity of statements from the interview transcriptions (Slover, 2007). Albalawi suggested that qualitative data can be analyzed using a variety of techniques such as transcriptions from audiotapes (2004) and this will lead to a better understanding of the research data (Slover, 2007). The researcher analyzed the qualitative

data through a description of emergent themes and also used comparative and contrastive methods in analyzing the data.

The data collected were purposely and thoroughly sorted and coded to gain insights and delineate anomalies and conflicting results (Slover, 2007). The purposeful sorting and coding of data implies that there is a reason in mind for this type of method to be selected (Creswell, 2003). A purposive technique is a method wherein one or more specific and predefined methods are used in the study for data analyses so that the researcher will understand the problem and answer the research questions (Creswell, 2003).

Analyzing the qualitative data from the interview process is a six-step procedure (Slover, 2007). This is shown in Table 9.

Table 9

Analysis of Qualitative Data Collected

Six Steps	Description
Step 1	Organize and prepare the data for analysis.
Step 2	Explore the data.
Step 3	Describe the data and search for patterns.
Step 4	Code the material by topic.
Step 5	Represent data and produce reports.
Step 6	Interpret the data and build theories grounded in data.

Note. From "A Case Study: Why Commercial Health and Fitness Facilities Achieve Defined Key Performance Indicators," By E. M. Slover, 2007, Unpublished doctoral dissertation, p. 86.

For the first stage, the researcher organized the data collected from the research log and the interview transcriptions and prepared them for examination. Each interview was analyzed independently and this permitted the researcher to gain a better understanding of the data. After this process, the investigator analyzed the transcriptions and notes in their entirety. This effort provided a general sense of the content and common themes and patterns, which became the source for the coding system utilized in the NVivo 7.0 software.

The second step in the process involved data exploration and further analysis of the content within the transcribed texts. The researcher focused on data importance to the research questions. This provided pertinent information in this stage of data discovery. The next phase involved the description of data and the search for patterns. An important characteristic of qualitative analysis is the resolution of data into the constituent components to reveal themes and patterns (Dominic, 2007).

As data were coded, patterns emerged, that were categorized in relation to the research questions and interview instrument (Appendix E). The categories that emerged were experience, purpose, safety, and exposure, because they related to ease of use; usefulness, security, and awareness, each of which addressed the research questions (see Figure 8). In Step 4, the data were entered into the Nvivo 7.0 software, which was used to analyze data collected from the one-on-one, semi-structured interviews. The data representation involved descriptions of themes uncovered in the investigation. The final step in the analysis of qualitative data was the interpretation and summarization of

emergent themes, which served as the basis to answer the research questions regarding the dynamics that influenced the implementation of biometrics technology for control of identity fraud within Nigeria.

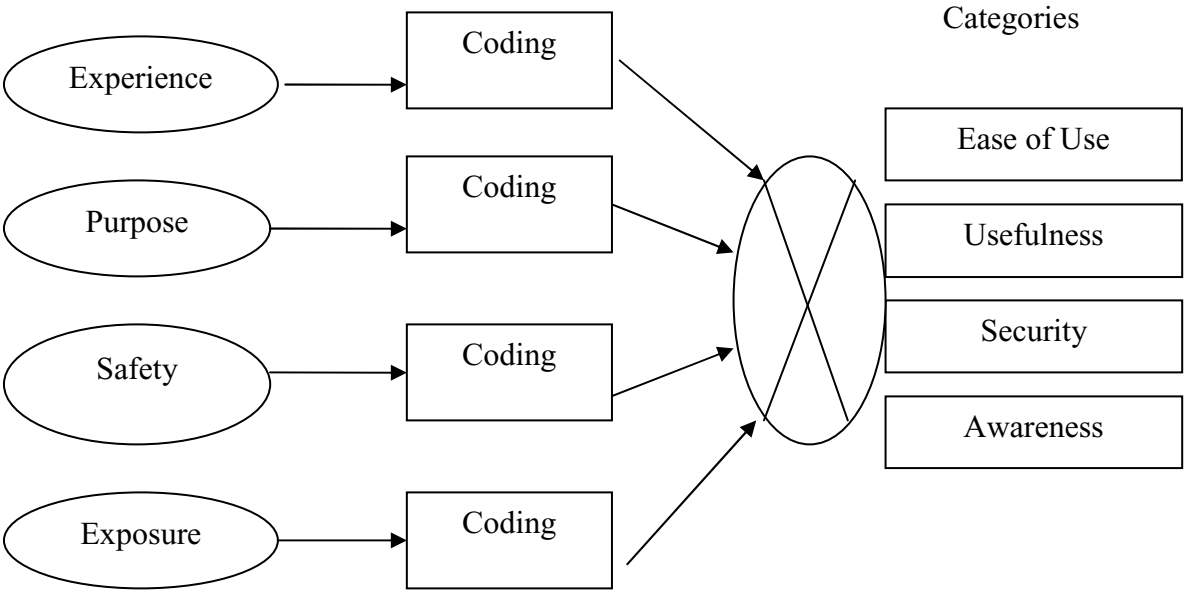


Figure 8. Categories of coding.

Emerged Categories

In Figure 8, experience, purpose, safety, and exposure emerged after coding, consolidation, and characterization of participants' responses to indicate their perspectives.

Experience. On the basis of coding, data consolidation, and comparative and contrastive methods in analyzing data, users' experience will influence implementation of technology. If users perceive that the use of biometrics technology is complex, then this will impact adoption because it is not easy to use. The technology acceptance model (TAM), which is the theoretical model for this study, states that users will implement technology due to ease of use. This can be attributed to users' experience, knowledge, and lack of complexity of the technology.

Purpose. From the coding technique and process, purpose is mapped to the category of usefulness of biometrics technology. The reliable identification of a person is a useful function of biometrics technology and serves the purpose for identity management. On the basis of coding, data consolidation, and comparative and contrastive methods in analyzing data, purpose is mapped to the category of utility and effectiveness of biometrics technology. Users will have the belief that biometrics technology will provide useful function of identity protection to be considered for adoption.

Safety. To address the issue of safety, the participants suggested that biometrics should provide security for the individuals in such areas as reliable identification, banking, and on-line transactions. In this case, the issue of safety, which mapped to security, was not mute as participants' responses indicated that security was a major issue. Therefore, participants considered safety, which mapped to security, as a category that will influence the implementation of biometrics technology for control of identity deception.

Exposure. The responses reported in this category were sorted from the answers to the four research questions. The respondents agreed that exposure to biometrics technology created knowledge or awareness that has a bearing on the implementation. This category, therefore, catalogs the concerns of how the exposure issue is exacerbated by the debate about awareness. Therefore, to be enriched by that knowledge of biometrics technology meant that individuals would benefit from the awareness mechanism. Over time, exposure, which translates to awareness, will influence interest in biometrics technology adoption for the control of identity deception.

Qualitative Presentation

Experts such as Creswell (2003) and Dominic (2007) recommended that researchers control the emergent categories and themes to manageable and analyzable units. This is very important for achieving accurate data description. In this qualitative component of the study, the perspectives of participants provided answers to the research questions that guided the study. The researcher presents the descriptive components that were filtered from the interviewees' responses related to the interview protocol (Appendix E).

The first research question was, "What is the relationship between ease of use and adults' perceptions toward adoption of biometrics technology for control of identity fraud?" The objective of this question was to determine if ease of use will influence the implementation of biometrics technology. If the technology for the identification and authentication of individuals is easy to use, then this will influence the favorable

perception toward adoption of the technology. On the other hand, if users perceive that they would have difficulty to use biometrics technology system, that will have a negative impact and participants will not be interested to favor adoption of the technology.

The participants were asked to reflect on their understanding of identity fraud as a threat to individual security, banking, and document forgeries. The data collected from Question 1 responses allowed the researcher to determine the relationship between ease of use and adults' perceptions toward adoption of biometrics technology for control of identity fraud. The researcher further explored and examined Question 1 from the responses through follow-up questions about specific aspects of ease of use that would influence the adoption of biometrics technology.

There were 20 participants, 11 (55%) were males and 9 (45%) females. The fewer the interview participants, the deeper the researcher made inquiry per an interviewee. This provided better interaction and richer responses from the participants. Of the 11 interview participants that were males, 8 (40%) indicated they would use biometrics technology if it was not difficult. The point these participants stressed was that if biometrics technology was easy to use, then they would use it. This factor represented an influence toward adoption of biometrics technology for credentialing identity to control safe banking, protect identity, and documents frauds within Lagos, Nigeria. On the other hand, 3 (15%) of male participants did not provide favorable opinion if ease of use of biometrics technology will influence their attitude for adoption.

Similarly, there were 9 (45%) of female participants. Out of this number, 7 (35%) female participants indicated that ease of use was a dynamic that would sway their perception for biometrics technology adoption. On the other hand, only 2 (10%) did not provide positive responses. The number of females (35%) who responded and agreed to the dynamics of ease of use as an influence was more than half of female participants. This was not surprising to the researcher; since females were more concerned about becoming victims of identity fraud (Stampel, 2009).

Overall, 15 (75%) of male and female interview participants from the total sample of 20 indicated that ease of use was a factor that would influence their behavior toward the adoption and usability of biometrics security system. These findings support the technology acceptance model (TAM) (Ngugi, 2005; Wahid, 2007), as revealed in the literature review, which serves as the theoretical model for this study. The TAM states that ease of use will influence users' perception toward adoption of technology. On the other hand, 5 (25%) of male and female participants had no favorable opinion for the research question. Figures 9 and 10 depict these findings.

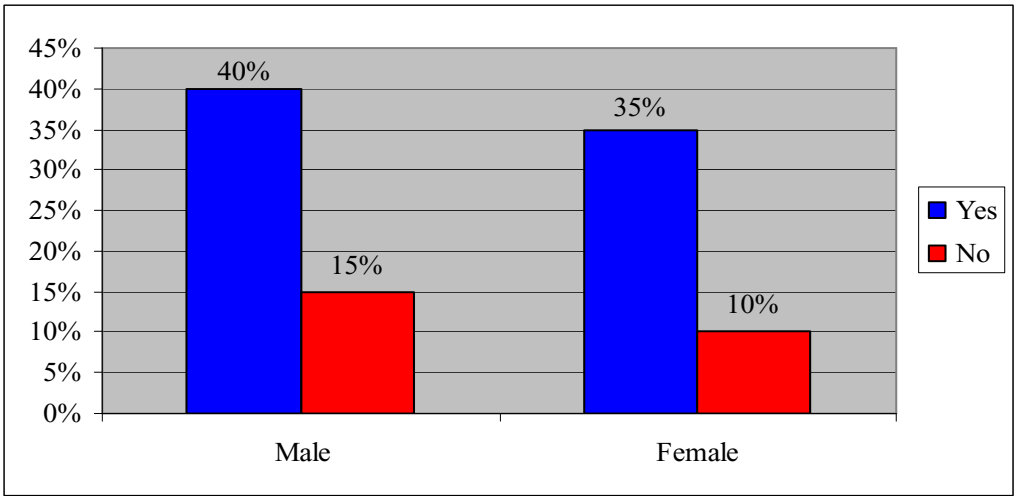


Figure 9. Male and female yes-no responses for Interview Question 1: Ease of use of biometrics technology as influence for adoption.

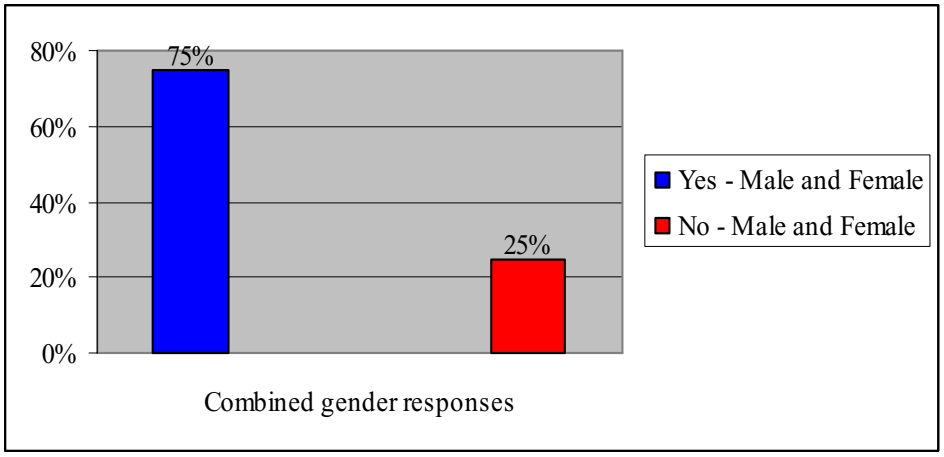


Figure 10. Combined gender responses for Interview Question 1: Ease of use of biometrics technology as influence for adoption.

The reliability of the identification of individuals is a useful function of biometrics technology. To address the issue of usefulness, the second research question asked, "To what extent, if any, is biometrics technique considered a reliable mechanism for identity verification, and what is the relationship between perceived usefulness and the acceptance of biometrics technology for control of identity deception?" Each of the

interviewees was asked this question in addition to follow-up questions. The information gathered from participants' responses allowed the researcher to examine and determine the system's effectiveness and usefulness as a dynamic that impacts the implementation of biometrics technology.

The analysis of the interview indicated that study participants believed the function of reliably identifying people is a useful utility of biometrics technology. However, they expressed concern regarding if there were errors in the system, for example, where an individual might be incorrectly identified (i.e., false identification). Biometrics technology errors have raised apprehensions (Acharya, 2006; European, Commission, 2005; U. S. Treasury, 2005). While the errors have resulted in considerable criticisms surrounding biometrics, many authors have realized the significant advantages as the technology has improved and is used for monitoring and controlling identity (Bocozk, Buster, Fitzgerald III, Vacca, Welsh, & Wulf, 2005).

To answer the second question, there were 20 participants, 11 (55%) were males and 9 (45%) were females. Of the 11 interview participants that were males, 7 (35%) indicated they would use biometrics technology for its usefulness because it is a mechanism to reliably credential identity. The participants were aware and also reported that fingerprint scan as identification techniques, which have been regarded as the 'grandfather' of all biometrics, was prevalent and effective and have been used for decades. It was a surprise to glean from the results that iris scanning was not popular compared to the fingerprint system. This will require major efforts to increase awareness,

promotion, and dissemination of information to counteract this perception. On the other hand, 4 (20%) of male participants did not agree that the usefulness of biometrics technology will sway their opinion for implementation.

For the female participants, the researcher recorded 6 (30%) who indicated the function of usefulness will affect their perception for adoption. Similarly, female participants indicated that the biometrics system has advantages over other methods of identification mechanisms. The female participants were familiar with fingerprint scan because of its application in crime investigation and prosecution. Although their interest in iris technology was reported, the females were not very familiar about its application and functionality.

On the other hand, 3 (15%) had no favorable responses. Overall, 13 (65%) of interview participants (male/female) indicated that the function of usefulness will affect their perception for biometrics technology implementation. This finding supports the technology acceptance model (TAM) (Ngugi, 2005; Wahid, 2007), which serves as the theoretical model for this study. The TAM stated that usefulness will influence users' attitude toward adoption of technology.

Conversely, 7 (35%) of the interview participants did not have favorable opinion about the interview question. Figures 11 and 12 show these findings.

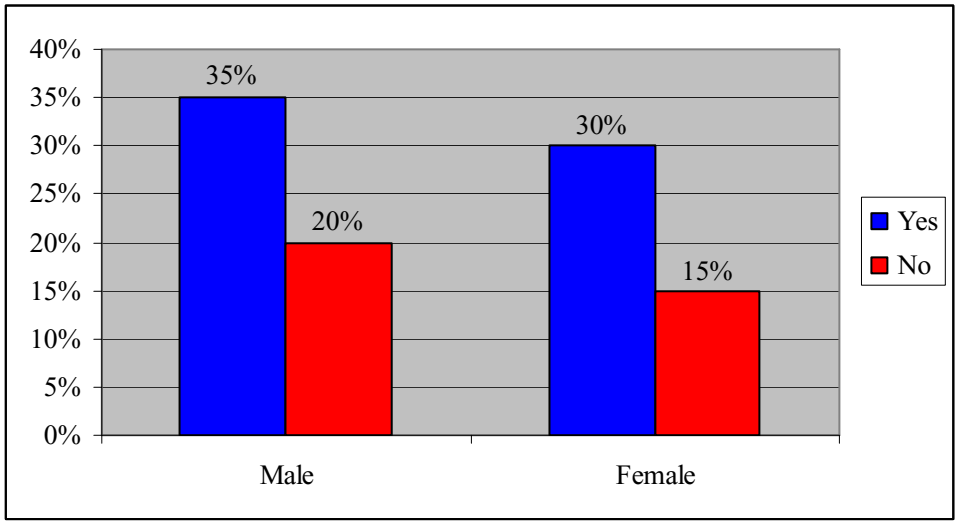


Figure 11. Male and female yes-no responses for Interview Question 2: Usefulness of biometrics technology as influence for adoption.

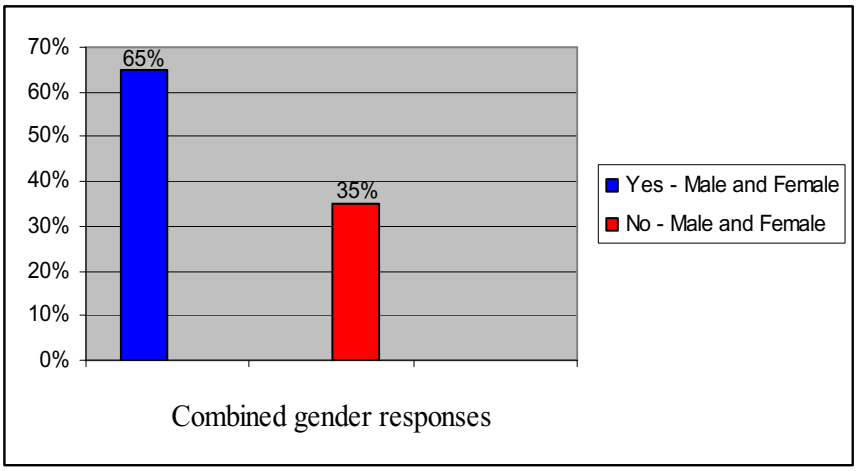


Figure 12. Combined gender responses for Interview Question 2: Usefulness of biometrics technology as influence for adoption.

The next question built on previous issues. The increase of identity fraud has raised concerns in developed countries (Gordon & Willox, 2003, 2006) as well as in developing countries such as Nigeria (Oghre, 2007). In addition, identity fraud has facilitated other crimes (Choo, Gordon, Gordon, & Rebovich, 2007). Similarly, the safety and security of individuals have been major causes of anxiety. To address this issue, the

third research query asked, “What is the relationship between security and adults’ perceptions toward adoption of biometrics security for control of identity fraud?”

The participants were asked how safety and security were important to them in relation to identity protection. The responses gathered from the participants reflected their opinions. This information permitted the researcher to determine the perception of the research subjects regarding security relative to the adoption of biometrics technology to control identification and authentication scams.

Identity fraud is a phrase that evokes security concerns, and biometrics systems have been recognized as preventing this type of crime through reliable identification. The participants’ responses proved the seriousness and concern about their identity theft and used in the commission of crime. Hence, the results of this question were not surprising to the researcher. About 9 (45%) of the male respondents, and 8 (40%) of female participants indicated they are apprehensive about their identity being stolen and were in support of the adoption of biometrics security systems.

The participants expressed their opinions and agreed that application of biometrics technology would help protect bank accounts from unauthorized access and compromise. Overall, significant majority 17 (85%) of the interview participants favored security concern as a dynamic that would influence their opinion about the implementation of biometrics technology. These findings supported the position of Koshy (2009), who concluded that perception of safety and security influenced users’ perception toward usability and adoption of biometrics technology. On the other hand,

only 3 (15%) of interview participants did not register favorable opinion. The findings are depicted in Figures 13 and 14.

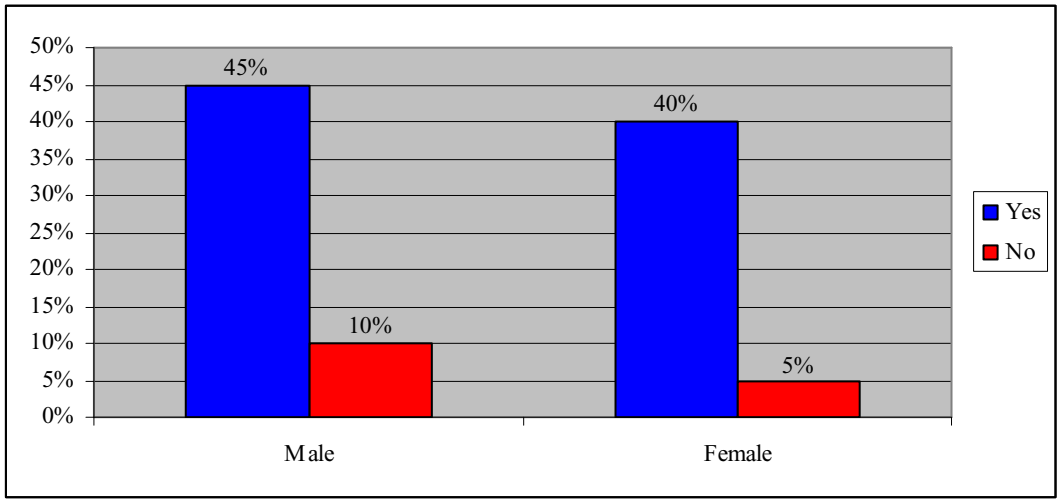


Figure 13. Male and female yes-no responses for Interview Question 3: Influence of Security Concern toward adoption of biometrics technology as influence for adoption.

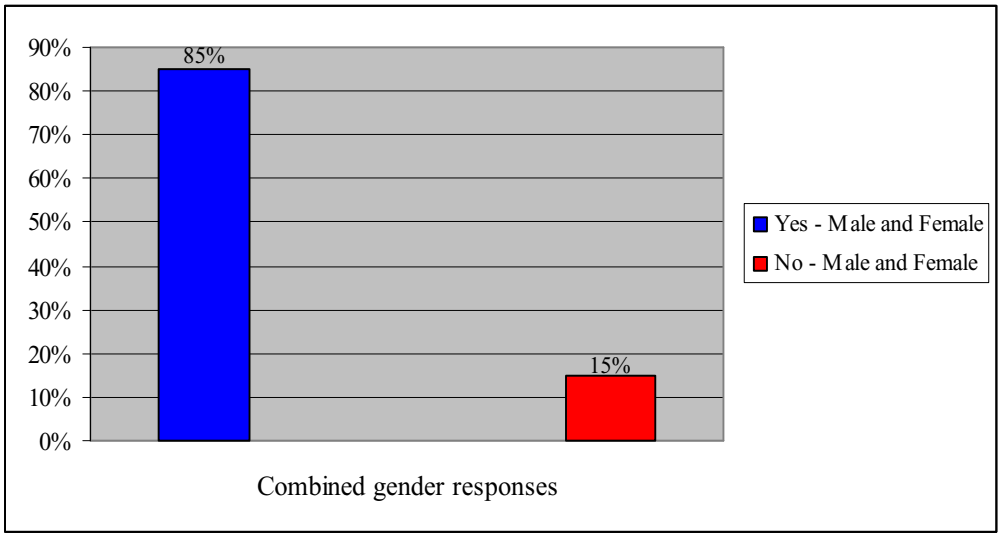


Figure 14. Combined gender responses for Interview Question 3: Influence of Security Concern toward adoption of biometrics technology as influence for adoption.

The last question was about awareness. Regardless of the possibility of ease of use, usefulness, and security, adoption of biometrics technology will be diminished

without awareness. As the literature review revealed, awareness was expected to bring changes in behavior and attitude toward biometrics technology adoption over time. It was necessary, therefore, that individuals were cognizant of biometrics technology and its ability to protect identity and maintain personal security.

Therefore, with respect to awareness, the fourth research question asked, "What is the relationship between adults' awareness and the adoption of biometrics technology for control of identity deception?" The majority of the participants indicated that they were aware of biometrics technology. The researcher found that the participants expressed interest in the policy that promotes the dissemination of information about the technology and its benefits.

Of the 20 participants, 10 (50%) of male and 8 (40%) of female participants indicated that awareness of biometrics technology was a factor that would impact their opinion toward adoption. Only 1 male participant (5%) and 1 female respondent (5%) for a sum of 2 (10%) did not consider awareness as a factor that would influence adoption of biometrics technology. In previous interview questions, the researcher did not record 90% response. In this particular question, the significant majority about 90% of the interview participants agreed that awareness was a major factor that would influence their perception for biometrics technology adoption.

The more adults were aware of the technology, the better informed about the functions and usefulness. This response was consistent with Asfaw (2006) who stated that awareness over time would influence adoption of technology while the constructs of

ease of use and usefulness were consistent with TAM (Ngugi, 2005; Wahid, 2007), which states that ease of use and usefulness will influence the use of technology. The findings of the awareness question are depicted in Figures 15 and 16.

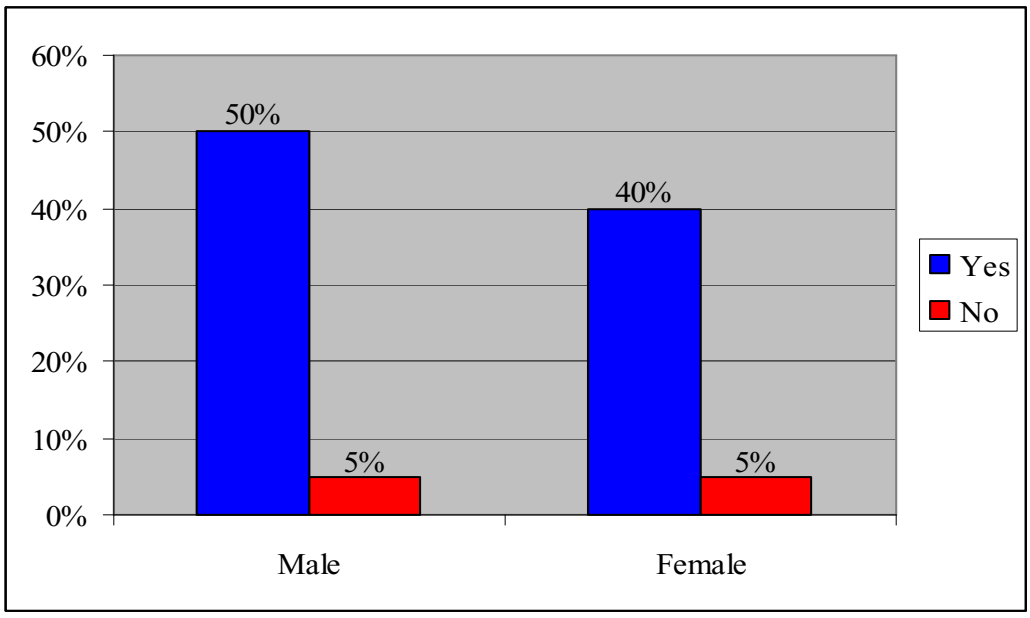


Figure 15. Male and female yes-no responses for Interview Question 4: Awareness of biometrics technology as influence for adoption.

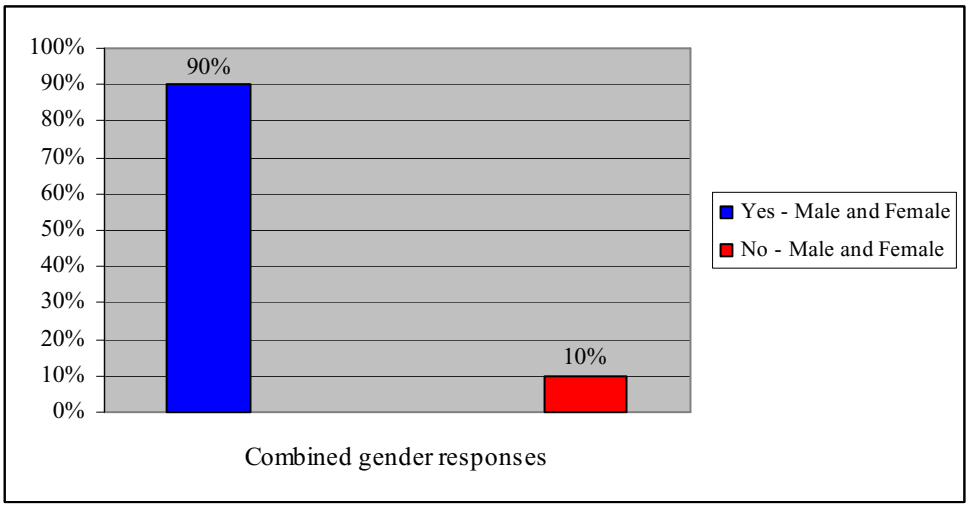


Figure 16. Combined gender responses for Interview Question 4: Awareness of biometrics technology as influence for adoption.

Findings and Emerged Themes from the Qualitative Component

The researcher noted with interest the participation from the research subjects for the qualitative phase of the study. Their concern about identity fraud and the growing interest in biometrics technology for mitigation was evident. The research questions sought to determine the dynamics that will influence the adoption of biometrics technology for control of identity fraud.

The analyses from the interviews suggest that the categories of ease of use, usefulness, security, and awareness are dynamics that would influence adoption of biometrics technology. The interview participants reported that ease of use was necessary to spur interest in the technology. The research subjects indicated that the complexity of the technology might intimidate users and that can discourage favorable opinion and behavior toward adoption.

The ability of the technology to reliably identify people for the purpose of individual confirmation was regarded as a useful function that will impact adult perceptions for implementation. The interview participants were concerned about the issue of security. The responses reflected the opinions of the research subjects, which suggested that security is a dynamic that will influence the adoption of biometrics technology for the protection of identity. The interview results also showed that awareness was as equally important as the other dynamics that were part of the research questions.

Some of the sample comments collected from the interview transcripts and log include the following:

- If biometrics technology is not complex to use, [the] majority of people will be interested to use [*sic*] it in banking transactions to protect financial records.
- Maybe this technology was needed to identify registered voters to avoid voter fraud. Biometrics technology will be helpful to manage [*sic*] identity and hold individuals responsible when they commit crimes.
- The implementation of [a] biometrics technique seemed to be a good idea but there must be awareness for [*sic*] the benefits so that people become familiar about [*sic*] it and develop favorable attitude[s] that will encourage its adoption.
- Practically speaking, I would tend to use the technology for the protection of my identity but worry if the biometrics data was stolen.
- I am concerned [about] what happens if the wrong person is not correctly identified and, as a result, the individual is allowed to have access to restricted data

In the next section, the emerged themes from the qualitative component of the study are discussed.

Emerged themes from qualitative component. Despite the findings, however, there were major themes that emerged from the interview. Such concerns were related to privacy, health, commercialization, and informationalization of human body into data. Some of the participants reported that biometrics technology may invade privacy if it is not properly implemented, secured, and administered. This problem can be attributed to the fear of the unknown syndrome. This concern has been a major criticism of biometrics technology (AlBalawi, 2004; Electronic Frontier Foundation, 2007). From the qualitative approach, the researcher categorized the concerns about privacy due to the following:

- The ability to monitor individuals without consent and knowledge. This is referred to as "Big Brother" (AlBalawi, 2004; Archarya, 2005; Lease 2005).
- Organizations and industries that gather biometrics data might commercialize the use.
- The fear of function creep: use of specific biometrics data collected for a particular use is exploited without either justification or authorization (Archarya, 2005; Lease, 2005). The typical example in this instance is the social security number used to identify social security recipients but later used as driver's license and other forms of individual identification. The social security number has been exploited for criminal activities such as identity fraud as a result of function creep.
- The difficulty of biometrics data substitution if there is a security breach of either the network or the database where data are maintained.

Another matter that emerged from the interview data was the issue of health. Concerns about health problems were a cause of apprehension among the adults that participated in the study. The adults raised the issue of cleanliness of the sensors used to capture data from fingerprint and iris scans. Although there have been no reports that confirmed any health issues associated with biometrics technology, the concerns of the participants in this regard warrants further scrutiny.

Such a situation can create unnecessary phobias about biometrics and, in turn, discourage adults from developing interest in the adoption and usability of biometrics technology for identity confirmation and control of fraud. The interview participants further expressed concern that organizations and industries that gather biometrics data might informationalize human body into data that can be manipulated, mismanaged, and only become machine-readable. Such practices might have the implication of the human body as readily available information in various aspects of life (Ploeg, 2005). In the next section, the quantitative analyses of the study are presented.

Presentation of Quantitative Component

The quantitative component of the study utilized a survey questionnaire instrument (see Appendix D) that was divided into five sections. The first section contained demographic questions. Sections 2 through 5 were designed to address individual research questions of the study. The questionnaire items in the sections were presented in a 5-point Likert–type scale so that the results could be quantified for the purposes of statistical analyses. The scale consisted of a series of representative

statements. The participants were asked to indicate agreement or disagreements in the form of strongly agree (5), *agree* (4), *no comment* (3), *disagre*e (2), and *strongly disagree* (1). This allowed the researcher to quantify participants' responses and provide a summation of values across each statement to give a total score for the participant. The numbers assigned were consistent with the meaning of the response.

The first section of the survey instrument contained items that addressed demographical information. In Section 2, there were nine items that addressed the question related to the ease of use of biometrics technology. There were five items in Section 3 that addressed the usefulness of biometrics security systems. In Section 4, there were ten items that addressed security concerns and the types of biometrics technology that are available such as fingerprint sensor and iris scan. Section 5 contained four items that addressed awareness regarding the adoption of biometrics technology. For the analyses and data interpretation, strongly agree was condensed to agree and strongly disagree was collapsed to disagree. The description of variables and demographical data are presented in the next following section.

Section 1 Description of Variables and Demographic Data

A total of 150 participants comprised the sample for the study. Out of the total sample of 150, 20 individuals were purposively selected and interviewed. The remaining 130 made up the available sample that was surveyed. The survey instrument was distributed directly to the research subjects at a centralized location. This provided the researcher the privilege to control the process. It also prevented the participants from

environmental and other undue influence. After the participants completed the questionnaires, the researcher collected the survey instrument. Of the collected questionnaires of 130, 10 were discarded because they were not correctly completed; they failed to meet the established criteria as defined in the study. The remaining sample called (N =120) was used for the analyses. The final sample denoted as (N = 120) consisted of 68 (n1, 57%) males and 52 (n2, 43%) females. The descriptions of the variables are presented next.

Description of variables. Below is the description of the variables:

Total sample of study = 150

Total sample used for interview = 20

Available sample for survey (150-20) = 130

Total number of survey instruments rejected = 10

Total sample used for the survey questionnaires (130 – 10) =120

N =120 participants in this study

n1 = 68 (number of males that participated in the study)

n1/N = 68/120 =57% of male participants in the survey

n2/*N* =52/120 = 43% (total number of female participants in the survey)

n1+*n2* = *N*, 68 + 52 = 120 (total number of survey participants)

n1 (57%) + *n*2 (43%) = 100%

In Figure 17, the gender statistics for the survey: n1=Males, 57%, n2=Females, 43%, are presented.

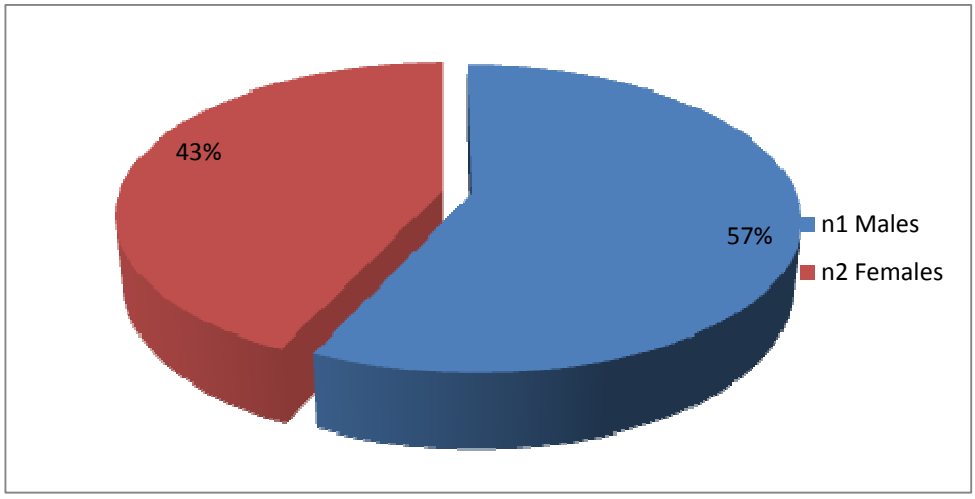


Figure 17. Gender statistics for the survey: n1=Males, 57%, n2=Females, 43%.

Table 10 provides the sample demographics of the survey participants in the study:

- The majority were males, 57%
- The percentage of females was 43%
- Most of the participants were between 41 and 60 years of age, 54%
- A higher percentage of both male and female were college graduates, 63%

Table 10

Frequencies: Demographics of Study Participants

	Frequencies
GENDER	
Male	57%
Female	43%
Total	100%
AGE	
Between 24-40	43%
Between 41-60	54%
Between 61-Over	3%
Total	100%
EDUCATION	
High School	28%
College Grad	63%
Masters/PhD	9%
Total	100%

Frequency Distribution of Reponses

Section 2 Results for Ease of Use

In this section, the frequency distributions of responses for the research questions are presented. The segment 2 results for ease of use as a dynamic that will influence the adoption of biometrics technology are discussed. The items in this section are part of "Research Question 1, (RQ 1)" of the instrument (Appendix D). There were nine items that addressed the question related to the ease of use of biometrics technology and included the following: I can personally use biometrics technology (RQ1. 1); I would feel

comfortable using biometrics technology (RQ1. 2); I could follow instructions easily to use biometrics technology (RQ1. 3); I would be able to use biometrics technology to protect my identity (RQ1. 4); using biometrics technology is far too complicated for me (RQ1. 5); I would like to use biometrics technology if it is not difficult (RQ1. 6); I would not use biometrics technology if it is complex (RQ1. 7); I would like instructions to be provided on how to use biometrics technology (RQ1. 8); and information about the system would help me make a decision to use it (RQ1. 9).

To answer the items of Research Question 1, the data were re-coded in Microsoft Excel, exported to SPSS, and analyzed to determine frequencies of participants' responses about the influence of ease of use toward biometrics technology adoption. Out of 120 participants, 69 (57%) for (RQ 1.1) disagreed and cannot personally use biometrics technology. On the other hand, 13 (11%) had no comment of personally using biometrics technology while 38 (32%) of respondents expressed interest to use. These data are presented in Table 11 and detailed in Appendix J.

Table 11

Frequency Distribution of Responses for Item 1 of Question 1

I can personally use biometrics technology					
		Frequency	Percent	Valid percent	Cumulative percent
Valid	Disagree	69	57	57	57
	No comment	13	11	11	68
	Agree	38	32	32	100
	Total	120	100	100	

Note: Percent summed up to 100 due to rounding.
All data about research question 1 items are presented in Appendix J: Ease of Use.

On Research Question1 the second item, (RQ1. 2); 53 (44%) survey participants disagreed of feeling comfortable to use biometrics technology while 6 (5%) had no comment. About half of the survey respondents 61 (51%) agreed of feeling comfortable to use biometrics technology. This is illustrated and detailed in Appendix J.

On the third item (RQ1. 3); 3 (3%) disagreed to easily follow instruction for the use of biometrics technology while 6 (5%) had no comment; and the majority of participants, 111 (92%) that responded expressed interest to follow instructions to use biometrics technology (see Appendix J). About the fourth item, (RQ1. 4); 30 (25%) participants disagreed to use biometrics technology to protect identity while 27 (22%) had no comment. About 63 (53%) agreed to use biometrics technology to protect identity. This is significant due to the usefulness of biometrics for security and identity verification and protection. The need to protect identity is increasing and biometrics technology is playing important role in identity management.

In (RQ1. 5); 26 (22%) of the participants that responded for the fifth item disagreed that using biometrics technology was far complicated while 10 (8%) had no comment. The majority 84 (70%) indicated that biometrics technology was too complicated. In the sixth item, (RQ1. 6); 4 (3%) of survey respondents disagreed to use biometrics technology if it is not difficult while 3 (3%) had no comment. On the other hand, 112 (94%) agreed to use biometrics technology if it is not difficult. This is significant and supported the theoretical model, TAM of this study. This model has been described several times in this paper. Adults will be hesitant to use technology that is

complicated and this can create technophobia, the fear or intimidation of using technology because it is complex or not easy to use.

For (RQ1. 7); 16 (13%) disagree they would not use biometrics if it is complex while 9 (8%) made no comment. On the other hand, 95 (79%) participants would not use biometrics technology if it is complex. This suggested that ease of use is very important for the adoption of biometrics technology. In the (RQ1. 8); only 2 (2%) disagree they would like instructions to be provided on how to use biometrics technology; while 5 (4%) did not have any comment.

A significant majority of the respondents 113 (94%) agreed that instructions be provided on how to use biometrics technology. On the last item (RQ1. 9); no respondent disagreed about information being helpful to make decision to use biometrics technology; while 1 (1%) respondent had no comment. On the other hand, 119 (99%) agreed that information about biometrics technology would be helpful to make decision to use and for adoption. If the participants' responses indicated the influence of ease of use, this will show that the usefulness of biometrics technology is of importance. Again, the Frequency Distribution of Responses for all items of research question1 is detailed in Appendix J. In the next segment, the researcher presents the results of section 3 about the participants' responses regarding the usefulness of biometrics technology.

Section 3 Results for Perceived Usefulness

The literature review revealed that reliability and perceived usefulness of biometrics technology to mitigate identity deception will influence adults' perception

regarding adoption and implementation. This section addresses "Research Question 2, (RQ2)," which was about biometrics reliability and perceived usefulness. There were five items: using biometrics technology to verify identity is a good idea (RQ2. 1); using biometrics technology to prevent identity fraud is a clever idea (RQ2. 2); I like the idea of using biometrics technology for identification (RQ2. 3); I would like to use biometrics technology to protect my banking transactions (RQ2. 4); and using biometrics technology as a reliable mechanism to identify criminals is a good idea (RQ2. 5).

Out of 120 participants, 8 (7%) participants that responded to (RQ 2.1); as shown in Table 12 disagreed that using biometrics technology to verify identity is a good idea while 5 (4%) had no comment. On the other hand, 107 (89%) agreed that using biometrics technology to verify identity is a good idea The data about the responses of all items for this research question are presented in Appendix K.

Table 12

Frequency Distribution of Responses for Item 1 of Question 2

Using biometrics technology to verify identity is a good idea					
		Frequency	Percent	Valid percent	Cumulative percent
Valid	Disagree	8	7	7	7
	No comment	5	4	4	11
	Agree	107	89	89	100
	Total	120	100	100	

Note: Percent summed up to 100 due to rounding.
All data about research question 2 items are presented in Appendix K: Perceived Usefulness.

For (RQ2. 2); 33 (28%) respondents disagreed that using biometrics technology to prevent identity fraud is a clever idea; while 49 (40%) had no comment. On the other hand, 28 (32%) agreed that using biometrics technology to prevent identity fraud is a clever idea. About the (RQ2.3); only 3 (3%) participants disagreed about the idea of using biometrics technology for identification. The majority of the survey respondents 112 (93%) liked the idea of using biometrics technology for identification; while 5 (4%) made no comment. For (RQ2.4); 40 (33%) disagreed of not using biometrics technology to protect banking transactions. About 34 (28%) had no comment; while 46 (39%) liked the idea of using biometrics technology to protect their banking transactions. The last item of this section is (RQ2.5). About 118 (98%) agreed that using biometrics technology to identify criminals is a good idea. On the other hand, only 2 (2%) had no comment. The researcher did not record any participant's response from data that were analyzed. Again, the Frequency Distribution of Responses for all items of research question 2 is detailed in Appendix K. In the next segment, the researcher presents the results of section 4 about the participants' responses regarding the security concern as an influence for the adoption of biometrics technology.

Section 4 Results for Security Concern

This section provides the results of "Research Question 3, (RQ 3)" about security concern with respect to the adoption and use of biometrics technology such as fingerprint and iris scan. The items of Research Question 3 included the following: I am not interested in using fingerprint technique for identification (RQ3. 1); I am not interested in

using the iris scan for identification (RQ3. 2); I have no need for fingerprint technology (RQ3. 3); I have no need for the iris scan (RQ3. 4); I would use biometrics technology to protect my identity (RQ3. 5); I can protect my identity without the iris scan security system (RQ3. 6); I would use fingerprint technology for banking services (RQ3. 7); I would use iris scan technology for banking services (RQ3. 8); I have been a victim of identity fraud (RQ3. 9); and I would like biometrics technology to be used to control identity fraud (RQ3. 10).

The analysis of the data for (RQ3. 1) showed that 120 (100%) of the participants disagreed for not having interest in using fingerprint techniques for identification. This result is presented in Table 13.

Table 13

Frequency Distribution of Responses for Item 1 of Question 3

I am not interested in using fingerprint techniques for identification					
		Frequency	Percent	Valid percent	Cumulative percent
Valid	Disagree	120	100	100	100
	No comment	0	0	0	0
	Agree	0	0	0	100
	Total	120	100	100	

Note: Percent summed up to 100 due to rounding.
All data about research question 3 items are presented in Appendix L: Security Concern.

In this instance, the majority of the respondents expressed the opinion of the need to use fingerprint scan for identification. The researcher suggests that the major reason for such majority response for this question reflects the need to reliably identify

individuals to prevent fraud and protect personal security. Fingerprint technology has been extensively and increasingly used in diverse environments (Chirillo & Blaul, 2003; European Commission, 2005; Nakashima, 2007; U. S. Treasury, 2005). It has been the oldest and most matured biometrics technology in use (Jamieson, Stephens, & Kumar, 2005). More importantly, fingerprint scan maintains a dominant market share in the biometrics technology industry (Lease, 2005; European Commission, 2005).

Of the 120 participants in the survey (RQ3. 2), 68 (56%) disagreed of no interest in using iris scan for identification. On the other hand, 26 (22%) had no comment while 26 (22%) agreed of having interest to use scan for identification. The majority of participants disagreed of having no interest to use iris scan for identification. In (RQ3. 3), 84 (70%) disagreed for having no need of fingerprint technology while 27 (22%) had no comment. On the hand, only 9 (8%) agreed of having no need for fingerprint technology. This responses suggest that majority of the participants indicated the need of fingerprint technology for use in detection or classification of identity.

The data for (RQ3. 4), showed that 58 (48%) disagreed of having no need for iris scan while 43 (36%) had no comment; and 19 (16%) agreed for having no need of iris scan. In this instance, the respondents are equally showing indication of the need for iris scan to be used for recognition.

For (RQ3. 5), the participants responded as follows, 10 (8%) disagreed the use of biometrics technology to protect identity. Similarly, 5 (4%) had no comment, and 105

(88%) agreed for the use of biometrics technology to protect identity. This shows there is need for adoption of biometrics technology for identification.

To understand (RQ3.6); 13 (11%) disagreed to protect their identity without iris scan. About 58 (48%) had no comment. On the other hand, 49 (41%) agreed to their identity without iris scan. The iris scan is one of the biometrics technologies that have not grown in popularity like the fingerprint scan. This partly may have influenced the survey participants' responses.

The literature review revealed growing concerns for the protection of banking assets of customers. The (RQ3.7) addressed that issue. From the data, 7 (6%) of survey participants disagreed they would use fingerprint technology for banking services. Similarly, 14 (12%) had no comment while 99 (82%) agreed they would use fingerprint technology for banking services. Fingerprint has long been regarded as the grand father of biometrics technologies (AlBalawi, 2006) and the survey participants' responses proved that.

The data for (RQ3. 8); showed that 50 (42%) disagreed they would use iris scan for banking services while 47 (39%) had no comment; and 23 (19%) agreed they would use iris scan for banking services. As the participants' responses show, about 19% agreed to use iris scan for banking services. Almost half 42% disagreed, which meant that most of the participants are interested to use iris scan for banking services. The education, awareness, and usefulness of biometrics technology must be addressed to help the respondents make informed decisions. According to Lease (2005), "The most important

strength of iris biometrics is its accuracy, the most critical weakness of facial scanning. Of all the leading biometrics, iris technology has the lowest error rate and the highest level of overall accuracy" (p. 41). This should spur interest in the use of this type of biometrics technology.

For (RQ3.9), 9 (8%) disagreed of being victim of identity fraud. About 54 (45%) had no comment. On the other hand, 57 (47%) agreed they have been victims of identity fraud. Identity deception has been a growing concern both in developed and developing countries. The implementation of biometrics technology has proven reliable both for identity management and verification of individuals.

The data for (RQ3. 10) showed that 118 (98%) agreed they would like biometrics technology be used to control identity fraud. Similarly, only 1 participant (1%) disagreed and 1 (1%) had no comment. The majority of survey participants agreed that biometrics technology is useful to control identity fraud. The literature review showed that biometrics technology is increasingly used to mitigate identity deception despite privacy concerns.

While ease of use, perceived usefulness, and security concerns are very important as dynamics that would influence adoption of biometrics technology, the impact of awareness is equally significant. The Frequency Distribution of Responses for all items of research question 3 is detailed in Appendix L. In the next segment, the researcher presents the results of section 5 about the participants' responses regarding the awareness as an influence for the adoption of biometrics technology.

Section 5 Results for Awareness

Regardless of ease of use, usefulness, and security, the possibility of encouraging the use and adoption of biometrics is significantly reduced without awareness (Asfaw, 2006; Norris, 2001). Awareness is very important as a factor that influences the adoption and usability of biometrics technology. The items in "Research Question 4, (RQ 4)" included the following: I have seen, heard, or read about biometrics technology such as fingerprint and iris scan (RQ4. 1), I have been exposed to biometrics technology such as fingerprint and iris scan (RQ4. 2), I am aware of the benefits of biometrics technology such as fingerprint and iris scan (RQ4. 3), and I know how biometrics technology can be used in daily life (RQ4. 4). The survey participants' responses are described below.

To understand (RQ4.1), 116 (97%) agreed of having knowledge about biometrics technology while only 4 (3%) disagreed. There was no survey participant that had no comment. This result is shown on Table 14 and more data for research question 4 are available in Appendix M.

Table 14

Frequency Distribution of Responses for Item 1 of Question 4

I have seen, heard or read about biometrics technology such as fingerprint and iris scan					
		Frequency	Percent	Valid percent	Cumulative percent
Valid	Disagree	4	3	3	3
	No comment	0	0	0	3
	Agree	116	97	97	100
	Total	120	100	100	

Note: Percent summed up to 100 due to rounding.
All data about research question 4 items are presented in Appendix M: Awareness

For (RQ4.2), the participants 63 (52%) agreed that they have been exposed to biometrics technology such as fingerprint or iris scan. About 20 (17%) disagreed and 37 (31%) had no comment.

The data for (RQ4. 3) showed that 61 (51%) agreed about how biometrics can be used in daily life. On the other hand, 30 (25%) disagreed while 29 (24%) had no comment. For (RQ4. 4); 78 (65%) agreed to know how biometrics technology can be used in daily life. Similarly, the participants' responses showed that 29 (24%) disagreed while 13 (11%) had no comment. The Frequency Distribution of Responses for all items of research question 4 is detailed in Appendix L.

To further answer the research questions, binary logistic regression, point bi-serial-correlation, and independent samples T-test were performed to determine the predictability of biometrics adoption and statistical significance of correlations.

Binary Logistic Regression, Dynamics of Influence, and Predictability of Biometrics Technology Adoption

As already stated, there were 120 participants in the study. A binary logistic regression was performed to understand the dynamics that would influence and predict adoption of biometrics technology. The binary logistic regression model contained 4 independent variables. All variables used a 1 to 5 scale where 1 was strongly disagree and 5 was strongly agree. The first independent variable was the ease of use scale which is an average score from nine questions associated with the ease of use of biometric technology.

The second independent variable was the perceived usefulness scale which was an average score from five questions associated with the perceived usefulness of biometric technology. The security concern scale was the third independent variable in the model, which was also an average score of 10 questions that focused on security concern. The fourth and final independent variable in the model was the awareness scale of biometric technology.

There were a total of 4 questions associated with the awareness of biometric technology that were used to derive the mean scores for the awareness scale. The dependent variable was adoption of biometric technology to control identity fraud. There were two possible responses to this question, yes I accept the adoption of biometric technology to control identity fraud or no, I do not.

The results indicated that the model was significant, χ^2 (4, N = 120) = 24.50, p < .01, and showed that the model was able to distinguish between respondents who indicated they would or would not adopt biometric technology to prevent identity fraud. The model explained between 18.5% (Cox and Snell R square) and 38.6% (Nagelkerke R squared) of the variance in biometric technology adoption, and correctly classified 94.2% of the cases. As shown in Table 15, perceived usefulness of biometrics technology made a unique significant contribution to the model, having a p value of less than .05 (.048) and an Odds ratio of 8.00

The next The Odds ratio is significant because for every unit increase in perceived usefulness score, the participants were 8 times more likely to accept adoption of

biometrics technology to prevent identity fraud. Therefore perceived usefulness would influence adoption of biometrics technology to prevent identity deception. The analysis the researcher conducted to determine the relationship among the dynamics and the adoption of biometrics technology was bi-serial correlation.

Table 15

Logistic Regression: Predicting Likelihood of Adopting Biometrics Technology

	B	S.E.	Wald	*df*	*p*	Odds Ratio	95% C.I. for Odds Ratio	
							Lower	Upper
Ease of Use	1.36	1.30	1.10	1	.29	3.91	.31	49.77
Perceived Usefulness	2.08	1.05	3.90	1	**.048**	**8.00**	1.02	62.94
Security Concern	-.39	1.14	.12	1	.73	.68	.07	6.33
Awareness	.62	.52	1.43	1	.23	1.86	.67	5.12
Constant	-11.57	5.14	5.07	1	.024	.000		

Bi-Serial Correlation: Relationship between Ease of Use, Perceived Usefulness, Security Concern, Awareness, and Adoption of Biometrics Technology

To further determine the influence of the dynamics, a biserial-correlation was conducted. A bi-serial-correlation is used for analysis when there are dichotomous variable (0 = no, and 1 = yes) and continuous variable (Varma, 2011). A biserial-correlation was conducted to assess the relationship between five variables, ease of use of biometrics technology, perceived usefulness of biometrics technology, security concern of biometrics technology, awareness of biometrics technology, and adoption of

biometrics technology. A biserial-correlation was performed because, the adoption of biometric technology variable in this analysis was a dichotomous variable (0 = no, and 1 = yes) and the remaining four variables were continuous. All of the variables used in this analysis were described in the logistic regression section. Table 16 contains a summary of the correlation results.

Table 16

Point-Biserial Correlation Among Ease of Use, Perceived Usefulness, Security Concerns, and Awareness

	Ease of Use	Perceived Usefulness	Security Concerns	Awareness
Adopt Biometric Technology	.38**	.41**	.12	.33**
Ease of Use		.28**	.32**	.28**
Perceived Usefulness			.28**	.54**
Security Concern				.25**

**p < 0.01

The results, as in Table 16, indicated that there was a statistical correlation between adopt biometrics technology and three other variables, ease of use ($r = .38$, $n = 120$, $p < .01$), perceived usefulness ($r = .41$, $n = 120$, $p < .01$), and (awareness, $r = .33$, $n = 120$, $p < .01$). This showed that the yes adoption group tended to believe that biometric technology was easier to use, more useful and also tended to have a greater awareness than the no adoption group. Ease of use was weakly correlated with perceived usefulness

($r = .28$, $n = 120$, $p < .01$) and awareness ($r = .28$, $n = 120$, $p < .01$), but had a medium correlation with security concern, $p = .32$, $n = 120$, $p < .01$.

This indicated that as ease of use scores increased perceived usefulness and awareness of biometrics technology scores also surged. Perceived usefulness was strongly correlated with awareness ($p = .54$, $n = 120$, $p < .01$), but not strongly correlated with security concern, $r = .28$, $n = 120$, $p < .01$, indicating that as increased scores in perceived usefulness accompanied by increased scores in awareness and security concern. Finally, security concerns had a correlation with awareness, $r = .25$, $n = 120$, $p < .01$ but not strong. This might be due to participants' indication of perceived usefulness, which is related to protection identity as a result of security concern. To assess mean score differences, sample t-test was also conducted.

Independent Samples *T*-test between Biometrics Adoption, Ease of Use, Perceived Usefulness, Security Concern, and Awareness

To assess if there were significant differences in scores on the composite scales of ease of use, perceived usefulness, security concerns, and awareness among those who reported they will adopt biometric technology and those who would not, four independent samples t-test were conducted. The dependent variable was biometrics technology adoption and the independent variables were ease of use, perceived usefulness, security concern and awareness. The independent samples *t*-test was conducted because the researcher wanted to assess the mean differences on 4 continuous variables between two groups (yes/no). The five variables used in these analyses have been described previously in this paper.

The results of the samples *t*-test is shown in Table 17 and figures 18-21. The independent samples *t*-test indicated that the yes adoption group ($M = 3.84$, $SD = .29$) had significantly higher mean scores on ease of use than the no adoption group ($M = 3.40$, $SD = .60$), $t\ (11.57) = -2.54$, $p < .01$, indicating that the participants agreed more that ease of use is a dynamic that would influence the adoption of biometrics technology. This is illustrated in Figure 18 and Table 17.

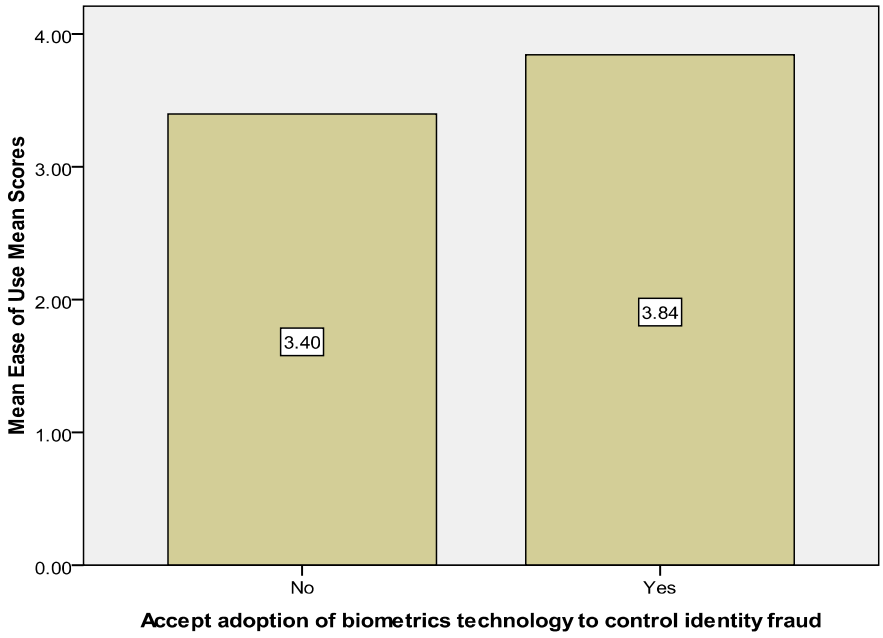


Figure 18. Mean scores of ease of use for adoption of biometrics technology.

The yes adoption group ($M = 4.10$, $SD = .46$) also perceived the biometrics technology to be more useful than the no adoption group ($M = 3.35$, $SD = .72$), $t\ (12.03) = -3.49$, $p < .01$. The data in Figure 19 shows mean scores of yes and no about perceived usefulness and Table 17 provides further information.

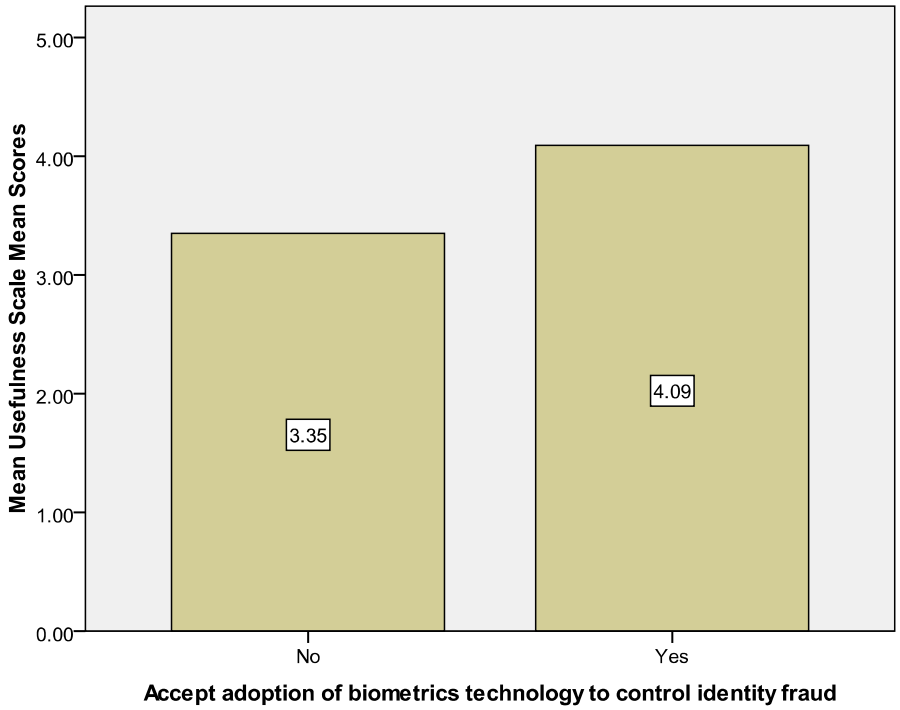


Figure 19. Mean scores of perceived usefulness for adoption of biometrics technology.

There were mean differences on security concern between the no subject group (M = 3.01, SD = .30) and the yes adoption group (M = 3.15, SD = .34), t (118) = -1.34, p = .16 and that is presented in Figure 20.

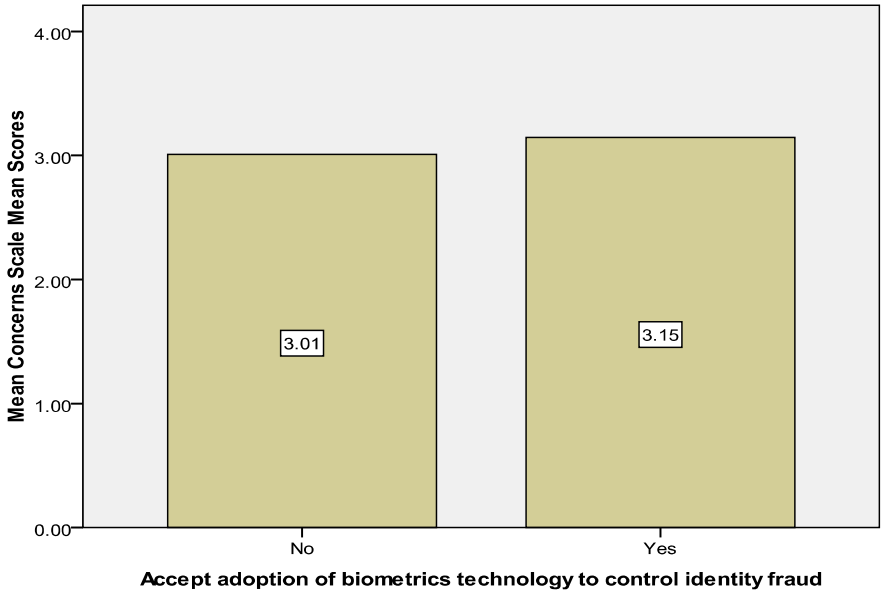


Figure 20. Mean scores of security concerns for adoption of biometrics technology.

Finally, the yes adoption group, (M = 3.92, SD = .73), t (118) = -3.81, $p < .01$ was aware of biometrics technology than the no adoption group (M = 3.06, SD = .87). This is illustrated in Figure 21.

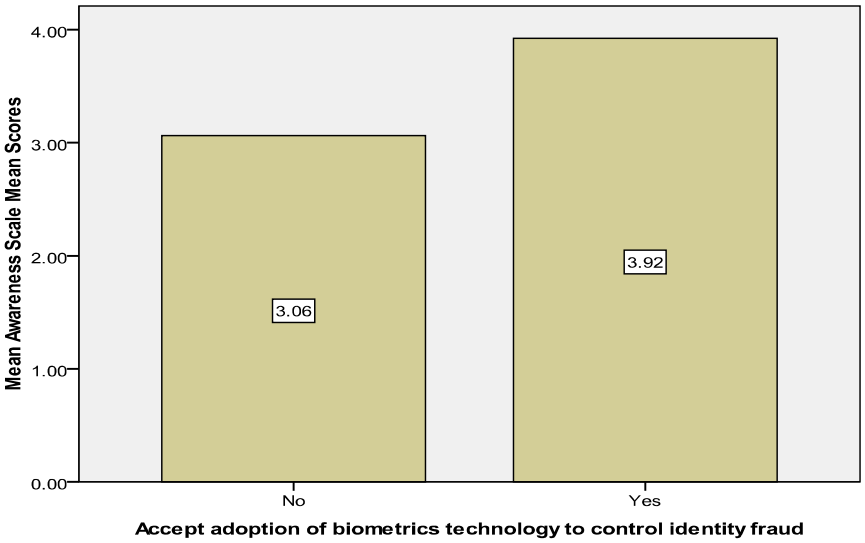


Figure 21. Mean scores on awareness for adoption of biometrics technology.

Table 17 shows detailed of mean scores of the dynamics that would influence adoption of biometrics technology. In the next section, further analysis that was carried out to determine if there were differences among the gender (dependent variable) and the dynamics (independent variable) that would influence adoption of biometrics technology is presented.

Table 17

*Independent Samples T-*test *between Biometrics Adoption, Ease of Use, Perceived Usefulness, Security Concern, and Awareness*

	Adopt Biometrics Technology Mean Scores		*t*	*df*
	No	Yes		
Ease of Use	3.40 (.60)	3. 84 (.29)	-2.54**	11.57
Perceived Usefulness	3.35 (.72)	4.10 (.46)	-3.49**	12.03
Security Concerns	3.01 (.30)	3.15 (.34)	-1.34	118
Awareness	3.06 (.87)	3.92 (.73)	-3.81**	118

Note. Numbers in parentheses are standard deviations.
**p < .01

Assessing Difference within Gender on Ease of Use, Usefulness, Security Concern, and Awareness

The researcher conducted an independent samples *t*-test to assess if there were gender (dependent variable) differences in the four mean composite scores of ease of use, perceived usefulness, security concern, and awareness (independent variables) (see Figure 22). The four independent variables used in these analyses have been described previously in this chapter. The independent samples t-test was selected for this analysis because the researcher wanted to assess the mean differences on 4 continuous variables between two groups (males and females).

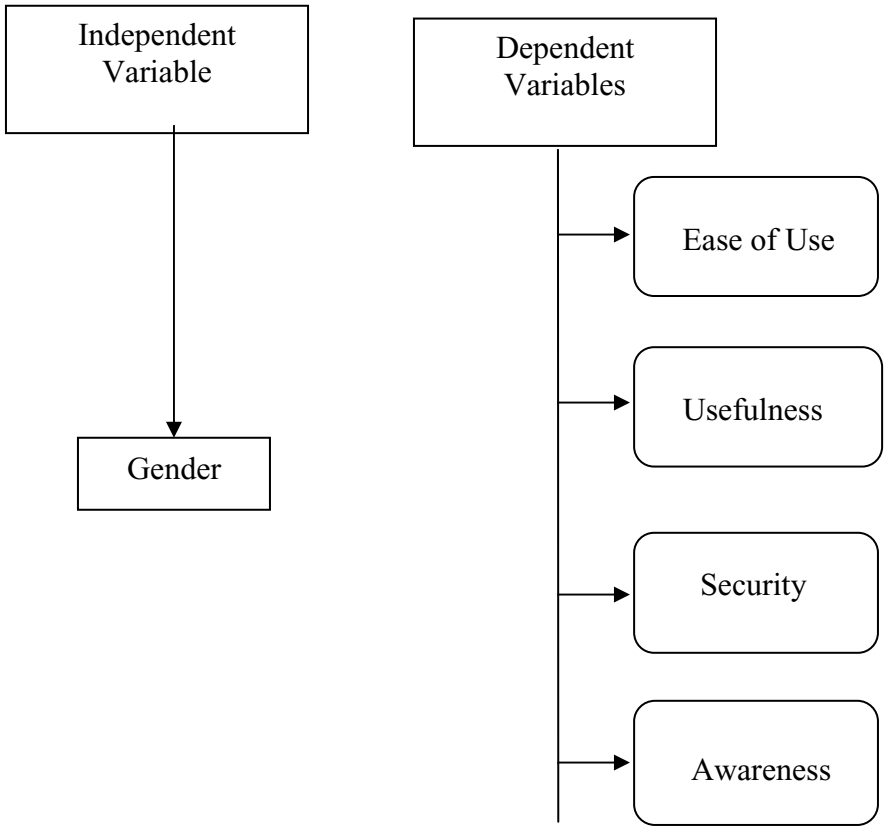


Figure 22. Assessing differences within gender on ease of use, usefulness, security concern, and awareness.

The results of the independent sample t-test are shown in Table 18 and Figures 23 to 26. From Table 18, there was a significant difference in mean scores on usefulness between females (M = 4.26, SD = .61) and Males (M= 3.83, SD = .39), t (81.40) = 4.47, p <.05. This indicated that females perceived biometrics technology to be more useful than males. This is shown on Figure 23.

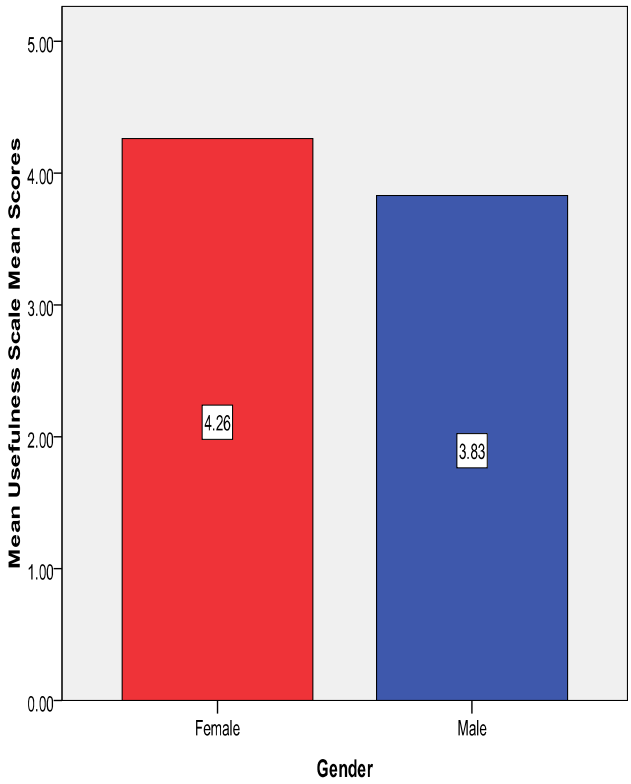


Figure 23. Mean scores on usefulness by gender.

This result suggests that females would rely on biometrics technology for control of crimes such as identity scheming, breach of bank, and credit card accounts (Unisys, 2005).

In addition, females ($M = 3.31$, $SD = .36$) had significantly greater security concern than males ($M = 3.00$, $SD = .25$), $t\ (86.77) = 5.28$, $p < .05$, as their mean scores on this measure were significantly higher. This is depicted on Figure 24. This result was not surprising because females were concerned about becoming victims of identity fraud (Stampel, 2009).

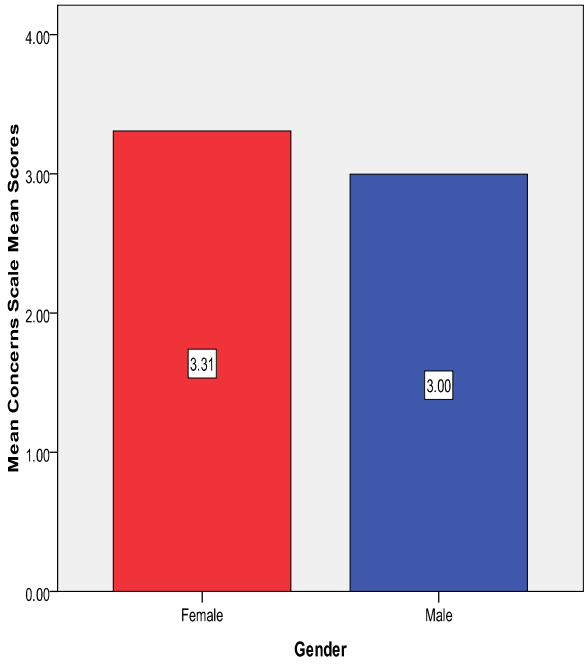


Figure 24. Mean scores on security concern by gender.

Females ($M = 4.00$, $SD = .78$) also had significantly higher mean scores on awareness than males ($M = 3.71$, $SD = .77$), $t\ (118) = 2.01$, $p < .05$, indicating that they had greater awareness of biometric technology to control identity theft. This is presented in Figure 25. This result implied that the adoption of biometrics technology will increase if more adults, particularly females, become aware of its role in crime mitigations.

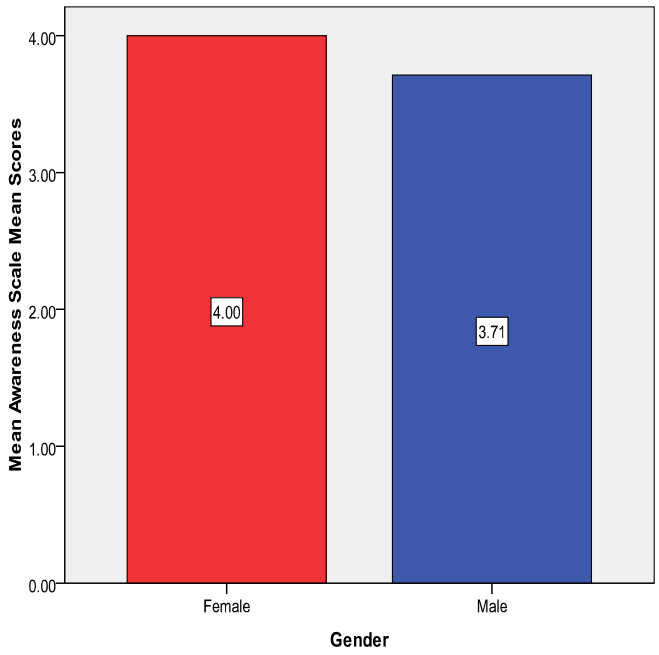


Figure 25. Mean scores on awareness by gender.

Finally, there were differences between males (M=3.83, SD = .33) and females (M = 3.76, SD = .39) on ease of use, t (118) = -.94, p = .35 but not significant. This is illustrated in Figure 26. One of the constructs of technology acceptance model (TAM) was ease of use, which has been referenced several times in this study. The ease of use will influence adults' perception and adoption of biometrics technology. In the next segment, the interpretation of the findings is presented.

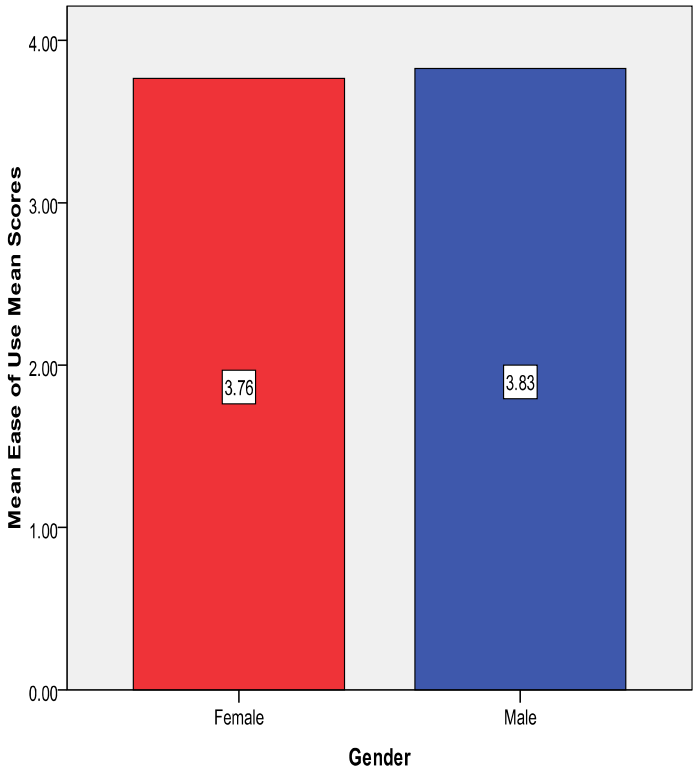


Figure 26. Mean scores on ease of use by gender.

Table 18

*Independent Samples T-*test *Between Gender, Ease of Use, Perceived Usefulness, Security Concern, and Awareness*

	Gender		*t*	*df*
	Female	Male		
Ease of Use	3.76 (.39)	3. 83 (.33)	-.94	118
Perceived Usefulness	4.26 (.61)	3.83 (.39)	4.47**	81.40
Security Concerns	3.31 (.36)	3.00 (.25)	5.28**	86.77
Awareness	4.00 (.78)	3.71 (.77)	2.01	118

Note. Numbers in parentheses are standard deviations.
**p < .01

Interpretation of the Findings: Quantitative Component

The data collected were analyzed using binary logistic regression, point-biserial correlation, and independent samples t-test. In this section, the interpretations of the results based on the items of the research questions are presented.

Interpretation of Findings for Research Question #1

Research Question #1 asked, "What is the relationship between ease of use and adults' perceptions toward adoption of biometrics technology for control of identity fraud?" The findings confirmed the following results: The analyses and interpretation of

Research Question #1 showed that a significant majority, 67% of participants responded and agreed that ease of use is a dynamic that will influence perception toward the adoption of biometrics technology. This is demonstrated in Figure 27.

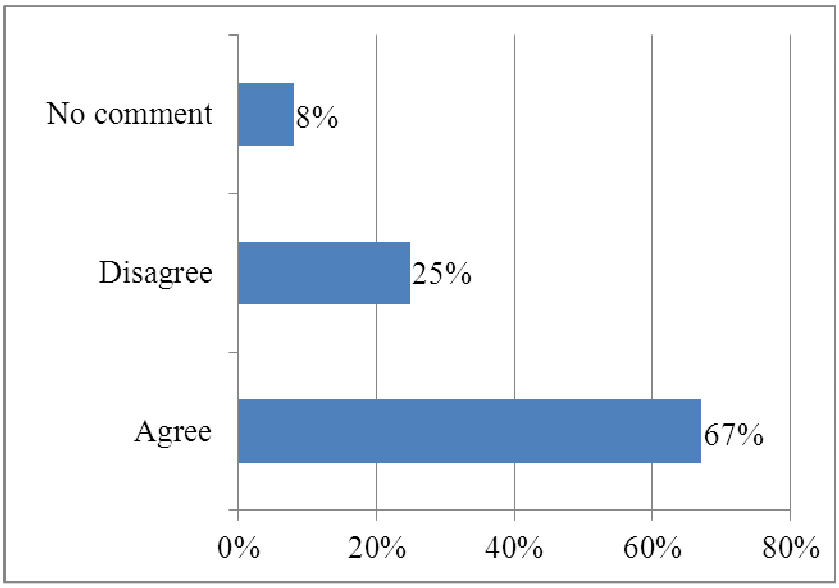


Figure 27. Summed up scores of Question 1 items: Ease of use.

This finding suggested that research respondents are concerned about identity fraud and protection of identity. The ability of biometrics technology to be used for reliable identity management may have contributed to the significant percentages recorded. The technology acceptance model (TAM), which was the theoretical model that guided this study, was also evidenced in this interpretation. The model indicated that the extent to which technology is implemented and used will depend on ease of use. From this finding, the participants indicated that if biometrics technology is easy to use, then a majority of adults will be able to use it, thereby avoiding the incidence of technophobia, which is the fear of adopting or using technology due to complexity or difficulty.

Interpretation of Findings for Research Question #2

Research Question #2 asked, "To what extent, if any, is biometrics technology considered a reliable mechanism for identity verification? And what is the relationship between perceived usefulness and the acceptance of biometrics technology for control of identity deception?"

The findings illustrated that participants in the study responded to the question in as reported in Figure 28. The findings for Research Question #2 show that 70% agreed that usefulness of biometrics technology will influence their behavior toward adoption. The technology acceptance model (TAM) stated that perceived usefulness, which was one of the constructs of the model, will affect adults' behavior for adoption. The findings from Research Question #2 demonstrated the influence of usefulness for the adoption and usability of biometrics technology.

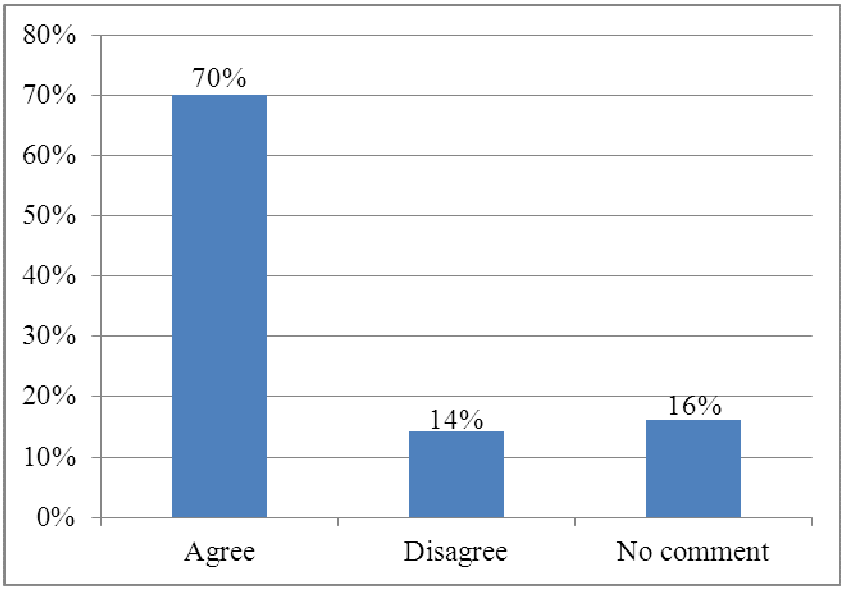


Figure 28. Summed up scores of Question 2 items: Perceived usefulness.

Interpretation of Findings for Research Question #3

Research Question #3 asked, "What is the relationship between security and adults' perceptions toward adoption of biometrics security for control of identity fraud?" The findings illustrated that adults who participated in the study answered the question in the following manner: about 42% agreed that security concerns will affect their perception toward adoption of biometrics technology; 7% more than the respondents that disagreed, and 19% more than the participants that had no comment.

This is depicted in Figure 29. An independent sample test that assessed any gender (dependent variable) differences in the four mean scores of ease of use, perceived usefulness, security concern, and awareness (independent variables) found that females had greater security concerns than males. This finding is not surprising since more women have become victims of identity fraud (Stempel, 2009) and the interest has increased to apply biometrics technology for authentication and identity management.

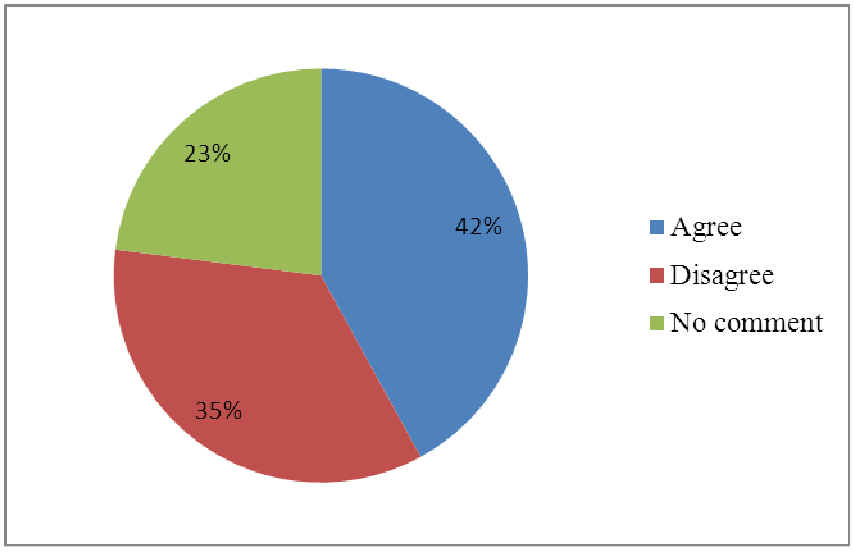


Figure 29. Summed up scores of Question 3 items: Security concern.

Interpretation of Findings for Research Question #4

Research Question #4 asked, "What is the relationship between adults' awareness and the adoption of biometrics technology for control of identity deception?"

The findings showed that 66% of participants responded and agreed as shown in Figure 30 that awareness was a factor that would influence their perception toward adoption of biometrics technology. While this is 49% more that the respondents who disagreed and had no comment, respectively, it suggests that dissemination of information to encourage behavior that will influence the adoption and usability of biometrics technology is very helpful. If adults are familiar or aware about the usefulness of biometrics technology, that will increase the likelihood of positive perception for adoption.

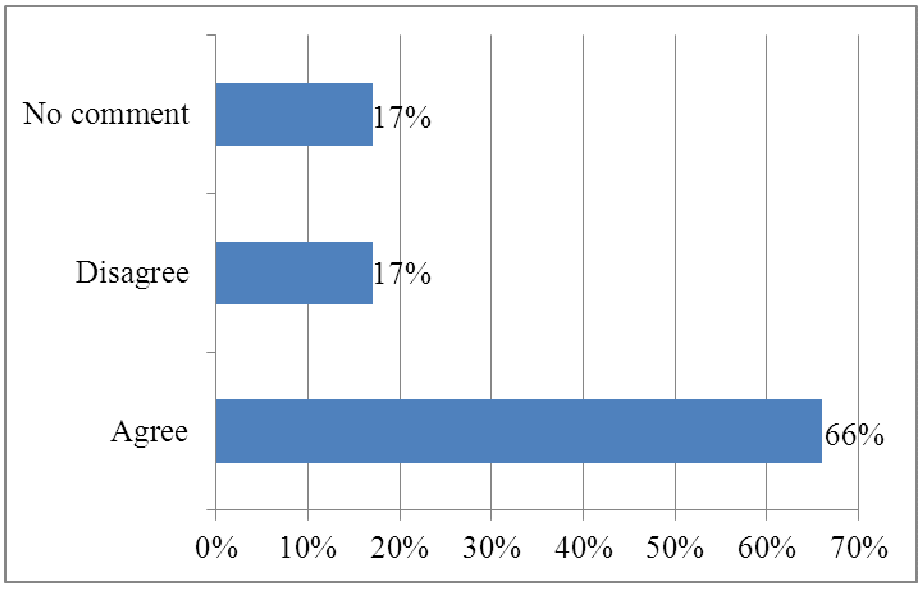


Figure 30. Summed up scores of Question 4 items: Awareness.

The outcome of the quantitative analyses will be compared with that of qualitative in the form of data triangulation, which is presented in the next section.

Data Triangulation

The purpose of data triangulation in this study was to strengthen the study findings and to confirm the outcomes of the research through different methods—qualitative and quantitative (Albalawi, 2004). In the process of data cross-checking and corroboration, the credibility of the research outcome is established. Albalawi (2004) suggested four different types of triangulation: "(1) data triangulation, the use of a variety of data sources in a study, (2) investigator triangulation, the use of several different researchers, (3) theory triangulation, the use of multiple perspectives to interpret a single set of data and (4) methodological triangulation" (p. 31). In this study, the researcher applied the fourth approach, methodological triangulation, which combines more than one method (qualitative and quantitative).

The interview (qualitative) and the survey questionnaire (quantitative) were two different data sources used in this investigation. Both methodologies complemented each other in this study. The survey provided broad representation but not a deeper understanding of the issues. However, the interviews provided more in-depth responses, but were not necessarily representative (Albalawi, 2004). In addition, the examination and verification processes ensured data reliability. Although each methodology was administered independently, the results of both approaches showed that the research participants in this study expressed autonomous opinions and answered the research

questions. In other words, the analyses of both methodologies indicated that ease of use, usefulness, security, and awareness will influence behavior toward the adoption and usability of biometrics technology for the control of identity fraud.

Treatment of Missing Data

Brydie (2008) stated that "several researchers have made specific suggestions pertaining to the management of missing data" (p. 76). The researcher may omit missing responses to specific survey questions if it is determined that their omission will not affect the validity of the statistical analysis (Brydie, 2008). For this study; the researcher omitted ten questionnaires as indicated in Section 1, Analysis of demographical data. The omitted questionnaires were rejected because the instruments failed to meet the established criteria as defined for the study. In this investigation, the researcher accepted no incomplete responses and determined that such omissions will not impact data analyses and the study results.

Comparative Analysis and Suitability of Methodology

The application of mixed methodology in scholarly research is a growing phenomenon. In this study, the researcher utilized an integrated method for which a qualitative approach was used to establish the basis of the investigation. Therefore, this study was qualitative and quantitative (Albalawi, 2004). The investigation started with a qualitative method and then a quantitative approach was used to complement the qualitative approach. This type of integrated strategy is termed "'Complementarity

Design' where findings from quantitative methods are enhanced through the findings from qualitative methods" (Albalawi, 2004, p. 25).

In this study, face-to-face interviews were used and became a major source of useful information during the investigation (Silverman, 2006). The interview was a direct meeting and interaction between the researcher and interviewees. A standardized interview instrument was used, where questions were asked of the respondents and the investigator later coded the participant's answers (Cano, 2009).

During the interview, the primary concern was to maximize the flow of valid, reliable information while minimizing distortions of what the interviewees knew. The interactional nature of the interview made the process unique, which was not true for the quantitative phase of the study. For instance, during the interview, the participants raised concerns about privacy and health issues. These were important findings that the researcher documented.

Although the interviews provided in-depth rejoinders, these were not necessarily representative of the study sample. On the other hand, representation was achieved with the survey for the quantitative approach though the survey did not provide a deeper understanding of the issues. In essence, the application of a mixed method strengthened this study as qualitative and quantitative data were combined to elucidate the complementary aspects and advantages of the integrated methodology (Albalawi, 2004).

Therefore, the suitability of the mixed methodology was justified in this study because:

- it increased data reliability and ensured a more comprehensive exploration of the research problems than would be possible using a single method, and
- it provided better answers that increased the robustness of understanding related to the research issues that were investigated

Summary

In chapter 4, the researcher presented the results of data analyses from the survey questionnaire and interviews. The goal was to answer four major research questions, as indicated at the beginning of this chapter. There were several types of analyses that the researcher conducted such as frequencies of response, binary logistic regression, point bi-serial correlation, content analysis, themes identification, and independent sample *t* test. The Microsoft Excel Spreadsheet, Nvivo computer software program, and SPSS were the tools used to analyze the data.

The analyses and interpretation of data showed that the participants in this mixed-methodology study expressed independent opinions that ease of use, usefulness, security, and awareness would influence the adoption and usability of biometrics technology for the control of identity fraud. A discussion of the results is presented in chapter 5. In addition, limitations of the study, implications for social change, conclusions from the study, and recommendations for further study are also presented.

Chapter 5: Summary, Conclusions, and Recommendations

Introduction

This purpose of the study was to examine the dynamics that would influence the adoption of biometrics technology for the control of identity deception within Lagos, Nigeria. The identified factors of influence used in this study were: perceived ease of use, usefulness, security, and awareness. This study was designed to determine the extent these factors will affect adults' behavior toward the adoption and usability of biometrics technology to protect identity and maintain personal security.

This study also assessed the technology acceptance model (TAM), which is the theoretical foundation for this research. This model shows that the extent to which technology is used will depend on factors such as ease of use and usefulness (Klopping & Mckinney, 2004; Ngugi, 2005; Wahid, 2007). Other authors stated further that security is a factor of influence (Brydie, 2008; Joshua & Koshy, 2009), while Norris (2001) stressed the importance of awareness.

In this chapter, the researcher provides summary, interpretation of the findings, conclusion, and further recommendations. The summary provides the focus of the study. Then, an interpretation of the findings and conclusions from the research questions are presented. The limitations as well as implications for social change are discussed. Finally, recommendations for action, further study, reflection, gaps in the literature, and concluding statement are presented.

Summary

The study focused on determining the dynamics that influence adult behavior toward the adoption of biometrics technology for the control of identity fraud. It is based upon the theoretical concept of the technology acceptance model (TAM). The study provides new data to individuals, businesses, government and its agencies, and technology manufacturers of biometrics devices, as well as researchers and scholars. More significantly, such data will help decision makers decide on the implementation of biometrics technology and the type of information and process of disseminating that information to gain public acceptance of this technology.

The perception of biometrics technology, its ability to protect identity, and the convenience of maintaining privacy are increasingly becoming more crucial to governments and businesses, as well as individuals. Correspondingly, these developments are apparent in the need to adopt and implement biometrics technology within the everyday lives of individuals. Consequently, it is imperative to investigate the factors, issues, or dynamics that influence interests in accepting biometrics technology as a mechanism for the reliable recognition of identity. If these dynamics are not properly considered and evaluated, the implementation of biometrics technology might result in project failure.

In this study, the researcher applied the mixed methodology approach that involved interview and survey strategies. These approaches were used to collect qualitative and quantitative data, respectively. The research instruments (interview and survey) contained several questions that were organized into six topics. The first theme

introduced the questionnaire and drew the socio-demographic profile and the status of the respondents' knowledge of biometrics technology through the use of a series of 10 questions. The second section related to the respondents' answers about ease of use of biometrics technology as an influence for adoption. There were a series of nine items. In section 3, there were five questions that examined the participants' responses regarding usefulness of biometrics technology and its impact on adoption.

The fourth theme assessed adults' responses about the relationship of security toward usability of biometrics technology and adoption through a series of 10 questions. The fifth topic focused on the respondents' awareness of biometrics technology as a factor of influence for adoption through a series of four questions. The last section drew responses from the interviewees using a series of four open-ended and follow-through questions. The results of the survey were presented in tabular forms.

Conclusions and Research Questions Answered

Biometrics technology has dramatically affected the identification, authentication, authorization, and accountability (IA3) of individuals after 9/11. The adoption and usability of the technology are transforming how identity is credentialed and also having positive social impacts. Economically, biometrics technology has generated several billions of dollars in revenue for the security industry and this growth is expected to continue as the demand for and reliability of identity management increase.

Socially, the implementation of biometrics technology for the identification of criminals and fraudsters has helped to maintain the record of 'social misfits' in the

database. This has made it possible to track and recognize individuals in the society who are involved in identity fraud. Politically, as the global war on terror (GWOT), money laundering to finance terrorism, and other criminal activities increase, biometrics technology serves as an appropriate tool for authentication and maintenance of individual identities. In border control, the technology has played a major role to prevent the influx of undocumented illegal aliens.

Although biometrics technology has gained a stronghold in developed countries, a review of the literature indicated that there is growing interest among developing nations, such as Nigeria, for the adoption and implementation of biometrics technology for the control of identity fraud. While developed countries benefit from the adoption and application of biometrics technology, emerging nations, for instance Nigeria, are removed from many of the social, economic, and political advantages of the technology. In this mixed methodology study, the researcher investigated the dynamics that will influence the adoption of biometrics technology for control of identity fraud and presents the following conclusions.

Conclusion from Research Question #1

What is the relationship between ease of use and adults' perceptions toward the adoption of biometrics technology for control of identity fraud?

- Quantitatively, a significant majority, 67%, of the research participants (see Figure 27, chapter 4) and the interpretation of findings from the analyses

conducted showed that ease of use is a dynamic that will influence adults' perceptions toward the adoption and usability of biometrics technology.

- Qualitatively, the findings and interpretation of data and interview responses results echoed the above conclusion.
- Overall, 75% of adults who were interviewed for this investigation (as illustrated in Figure 10, chapter 4) confirmed that ease of use of biometrics technology would influence adoption.
- Therefore, and based on these facts, the conclusion is that ease of use of biometrics technology is a factor that will affect adults' behavior toward the adoption and usability.
- This conclusion mirrors the body of literature reviewed in chapter 2 and the outcome of the qualitative component of this study.

In the literature, ease of use was a factor that will influence the acceptance and adoption of biometrics technology. The favorable user behavior towards adoption and usability is, in part, a function of ease of use.

The inference further confirmed the technology acceptance model (TAM), which is the theoretical model that guided this study. According to the model, adults will develop interest in using this technology if it is easy to use, thereby minimizing phobia (fear) among the users. On the other hand, the difficulty of biometrics technology will cause adults to lose interest in implementation. This will create technophobes—those adults that are afraid or fearful of using biometrics technology despite its usefulness.

The difficulty of the technology will dampen interest and affect adoption and usability. From this conclusion, it is inferred that ease of use is a dynamic that will influence adults' behaviors toward the adoption and usability of biometrics technology. This conclusion has also answered Research Question #1.

Conclusion from Research Question #2

To what extent, if any, is biometrics technology considered a reliable mechanism for identity verification? And what is the relationship between perceived usefulness and the acceptance of biometrics technology for control of identity deception?

The mechanism of reliability is a useful function of biometrics technology that will influence adults' behavior.

- Quantitatively, a significant majority, 70%, of the participants (see Figure 28, chapter 4) agreed that perceived usefulness will influence adults' perceptions toward the adoption and usability of biometrics technology.
- The SPSS analysis showed the Odds ratio indicated that for every unit increase in perceived usefulness score, respondents were 8 times more likely to accept adoption of biometrics technology to prevent identity fraud.
- A *p* value of .048, which was less than .05 and statistically significant, was recorded for perceived usefulness during SPSS analysis.
- The interpretation of findings of the analyses supported stated fact.
- The SPSS analysis indicated mean statistical significance among participants for yes adoption group ($M = 4.10$, $SD = .46$) for perceived usefulness of biometrics

technology more than the no adoption group ($M = 3.35$, $SD = .72$), t (12.03) = -3.49, $p < .01$.

- Qualitatively, the findings and interpretation of data and interview results supported the points.
- Overall, 65% of adults who were interviewed for this investigation (as illustrated in chapter 4, Figure 12) confirmed that perceived usefulness of biometrics technology would influence their perception adoption.

In this conclusion and based on the quantitative and qualitative analyses of the research data and the interpretation of findings in chapter 4, a significant majority of adults that participated in this study agreed that usefulness of biometrics technology will influence their perception toward the adoption and usability. This is consistent with the review of the literature and the technology acceptance model. The usefulness of technology is the second construct of TAM as depicted in Figure 4 in chapter 2. This theoretical model showed that the usefulness of technology will influence adults' interest and behavior in the adoption and usability of the technology.

Therefore, the conclusion is that a willingness among adult males and females to use biometrics technology is partly based on its usefulness. The notion of 'how does it benefit me' is very much at play in this instance. The usefulness of biometrics technology has been recognized in the hotel and banking industries, information technology sectors, in government and its agencies, and in educational course delivery systems, as well as in security and in the verification of identities. When biometrics technology is used to

reliably confirm the identity of a fraudster, its usefulness is not questioned or in doubt. From the above discussion, this conclusion has therefore answered Research Question #2.

Conclusion from Research Question #3

What is the relationship between security concern and adults' perceptions toward adoption of biometrics technology for control of identity fraud?

Security is a significant factor of concern that will affect users' interest, intentions, and actual use of biometrics technology (Jahangir & Begum, 2008; Joshua & Koshy, 2009). This is not a surprising statement due to increase in national and global trends of identity fraud, Internet frauds, terrorism, and border control problems. Biometrics technology is used to address the issues of authentication and validation of identity. Based on the responses and analyses of the quantitative component of this investigation:

- 42% of adult participants agreed that security concerns will influence their behavior toward the adoption and usability of biometrics technology (see Figure 29, chapter 4).
- 7% more than respondents who disagreed and 19% more than the participants who had no comment.
- 85% of interview participants indicated that security is a factor that will seriously influence their behavior toward adoption and usability (see Figure 14, chapter 4).

- For the interviewees, personal security and the protection of banking transactions and assets were areas of concern for, which biometrics technology can be used to mitigate victimization.
- These findings supported the position of (Koshy, 2009), who concluded that perception of safety and security influenced users' perception toward usability and adoption of biometrics technology.
- Based on the quantitative and qualitative data analyzed and recorded, it is therefore inferred that security concern is a dynamic that will influence adults' behavior toward the adoption and usability of biometrics technology.
- This conclusion has answered the Research Question #3.

Conclusion from Research Question #4

What is the relationship between adults' awareness and the adoption of biometrics technology for control of identity deception?

The literature reviewed in chapter 2 highlighted the importance of awareness in the adoption of technology and biometrics is no exception. Awareness is a dynamic that will influence behavior and affect usability. The quantitative result of this question indicated that:

- 66% of participants agreed that awareness of biometrics technology will influence their behavior toward adoption and usability (see Figure 30, chapter 4).
- 49% more than the respondents that disagreed and participants who had no comment, respectively.

- 90% of interview participants also agreed that awareness of biometrics technology will affect their perception toward adoption (see Figure 16, chapter 4).
- The SPSS analysis showed that increase in awareness correlated to ease of use.

The responses from the interview participants confirmed that it is difficult to determine the usefulness and security advantages of biometrics technology without awareness of the system. This suggests that dissemination of information is essential to encourage behavior that will influence the adoption and usability of biometrics technology. Consequently, the conclusion from this result is that awareness is a factor that will sway adults' behavior toward adoption and usability. This inference has answered the Research Question #4.

The primary results and responses from this research confirmed that ease of use, perceived usefulness, security concern, and awareness are the dynamics that will influence the adoption and usability of biometrics in Surulere, Lagos, Nigeria. In light of the study, this researcher emphasizes that these factors have an impact on the implementation of biometrics technology for the control of identity deception and the credentialing of individuals. The need for the adoption and usability of biometrics for identity management in Nigeria is clear as evidenced in the results and findings of this study. The researcher suggests that for the successful implementation of biometrics technology, project managers, stakeholders, policy makers, businesses, and biometrics vendors as well as the Nigerian government and its agencies should seriously consider

these dynamics to minimize failure of completion and application. In the next section, the author discusses limitations of the study.

Limitations of the Study

This study was conducted without limitations. This investigation concentrated on the following factors: ease of use, usefulness, security, and awareness. The concerns regarding privacy were not included or addressed in the study. In all likelihood, the answers to the research questions would have been affected. Adults will resist privacy intrusion. There is an opportunity cost between the issue of privacy and security. If privacy is emphasized, there will be less security. On the other hand, the more security is stressed, the less privacy.

There was no effort to determine the presence of biometrics vendors in Lagos, Nigeria, to determine the factors that influenced biometrics adoption. Such information would have been helpful for evaluating the findings of this study against the information from the vendors.

The technical experience of the participants presented a limitation when compared to similar samples in developed countries. The technical understanding of the functionality of biometrics is very important and as such will impact participants' responses. This was a limitation.

The availability of funds was another source of limitation. It was difficult for the researcher to conduct investigations beyond the budget of funds and time. In addition, this study was conducted during the rainy season in Lagos, Nigeria. This presented

communication and logistical barriers, hence, another limitation. The implications for social change are discussed in the following segment.

Implications for Social Change

Identity fraud has become a significant problem ravaging personal security and social and economic activities. The social implications of this study result from the identification of biometrics technology as a reliable and acceptable mechanism for the verification of a person, deterrence of identity deception, and protection of personal security. Identity fraud, however, may not be the only or even pressing national and international concern for mitigation. Crime is an impediment to economic and social stability. For a government to bring about positive social change, the unrest in the society resulting from law-breaking and its consequences must be addressed.

There is little argument about the fact that the economic and political strength of a country affects its social stability. The control of criminal offenses provides a favorable environment for economic growth and social stability. As the global war on terror (GWOT), identity fraud, money laundering, and other criminal activities continue to intensify, nations such as Nigeria will have the social responsibility to control them due to domestic and global consequences. Biometrics technology serves as an appropriate tool for the authentication and maintenance of identities. The technology will also ensure that criminals are correctly identified and that legitimate persons can maintain authorized access to secured sites, bank accounts, and other privileged areas.

Mitigating the concerns of adults will spur Internet and eCommerce activities. Many prospective marketers and consumers are reluctant to engage in cyber-economic transactions due to the growing trend of identity fraud. This crime has earned Nigeria a lot of negative global publicity. This, in return, has hampered investment from multinational corporations and foreign investors, which also impacts economic development. Biometrics technology is seen as providing a reliable authentication mechanism for identity management.

The results of this research will help the Nigerian government develop actionable strategies to implement and maintain a biometrics database. This will serve to credential identity and preserve the record of individuals who committed crimes. Another area that the technology has considerable influence is with the identification of voters. The rigging of voter registration is a growing concern in Nigeria every election cycle. Biometrics technology can be applied in identity management so that only registered voters who are verified in the biometrics database will be eligible to vote.

The security industry will also benefit from the results of this study. There is a growing need for data protection and access privileges of users and employees. Few identification, authentication, and accountability mechanisms, such as password and personal identification number (PIN), surpass the reliability of biometrics technology (AlBalawi, 2004; Harris & Yen, 2002). A biometrics security system has the capacity to confirm the presence of a person and potentially reduce the chances of identification

fraud (Coventry, 2005). In this instance, security is maintained and reliable identity recognition is improved and enforced.

This study investigated the dynamics that will influence the adoption of biometrics technology. The aim was to draw attention to the factors that will encourage the implementation and usability of biometrics for identity management. The identification of these dynamics will help the public as well as the private sectors to prepare and execute biometrics technology projects for the control of identity fraud. Finally, the adoption and usability of biometrics technology should be regarded from the following perspectives:

1. From an individual perspective, biometrics security system will promote positive social change. The rate of forgery and duplication of other peoples' documents is alarming. Biometrics technique will protect individual security and ensure that records belonging to an individual can be reliably verified. For instance, there is a growing concern regarding counterfeit banking documents and, in most cases, these are not identified as being phony. This results in fraudulent banking transactions that leave unsuspecting individuals vulnerable and victimized.

2. From the perspective of the general public, the widespread adoption of biometrics technology provides a substantial mechanism for mitigating a 'social cankerworm'—identity fraud. There is considerable, untapped potential in the country for domestic economic activities and foreign investment to achieve sustainable growth in the long run. Moreover, the negative publicity that identity fraud (IDF) generates about

Nigeria can be minimized if not eliminated in the global sphere. As a result, the widespread implementation and usability of biometrics technique will bring about positive social change in Lagos, Nigeria. In this section, the study's implications for social change have been addressed. The recommendations for action are presented in the following section.

Recommendations for Action

Participation among the stakeholders (society, government and its agencies, businesses, and individuals) requires alliances and partnerships for the actualization of the advantages accruing from biometrics technology adoption and execution. The results of this investigation suggest that relevant action is required among these stakeholders to enable the extensive and successful adoption and use of biometrics technology within Lagos, Nigeria. This will serve as a model for other states, major commercial cities, and the country as a whole.

The results of this study highlight the need for the development of an integrated national policy. The policy development process should encompass a broad range of stakeholders to gain input that will help to formulate actionable strategies for disseminating information about the need to control identity fraud on a national level. This process can take the form of a legislation enactment that encourages and supports the adoption and usability of biometrics technology for identity verification. Such efforts will help ease apprehensions about crime and assure citizens that measures are being undertaken to control criminal activities.

Improving acceptance of this technology and the role of biometrics security system for identification and authentication will require awareness. It is necessary to publicize the increasing need for biometrics technology for identity management. However, this will not be possible without significant and concerted efforts to inform and educate the stakeholders as well as the public. One major impact of awareness is the ability to influence behavior over time.

The role of media to inform the general public cannot be underestimated. This will include partnering with media outlets and journalists for the effective promotion and dissemination of information about biometrics technology relative to identity management and the control of forgeries and other types of deceptions. Similarly, workshops should be organized to educate people and raise awareness about the growing tendency of identity fraud and the function of biometrics technique as a control measure.

While policy, awareness, and partnership with the media and journalists are all important, allocation of resources is also required and necessary. For instance, the need for experienced and qualified human power to train and educate adults about biometrics technology is very important. Moreover, the provision and availability of financial resources are very critical to the success of implementing and adopting biometrics technology. The suggestions for action discussed in this section will be effective if implemented because adults are concerned about identity fraud and the results of this study proved it. In the next section recommendations for further study are presented.

Recommendations for Further Study

This study focused on the dynamics that will influence the adoption of biometrics technology in Lagos, Nigeria, a developing country in Africa. The study concentrated on factors such as ease of use, usefulness, security, and awareness. This could be a starting point for subsequent studies to provide a comprehensive understanding of biometrics technology as a verification mechanism used to credential individuals and control identity deception. A focus for future research could be privacy. While there is an increasing interest in protecting identity, there is the concern of privacy, in particular, in developed countries (Archarya, 2006; Baird, 2002; Newton & Woodward, 2001; Vollmer, 2006). The adults in developing countries such as Nigeria are no exception.

There are several biometrics modalities—among them are fingerprint, iris, face, and voice. The study of fingerprint can be carried out to determine if there is a preference compared to other types of biometrics techniques. For instance, the fingerprint scan is regarded as the grandfather of all biometrics systems. It has been used in law enforcement over the past 100 years and has become the de facto international standard for the positive identification of individuals (Jamieson, Stephens, & Kumar, 2005). A future study might focus on adults' willingness to adopt fingerprint technology in the effort to control identity fraud relative to other biometrics modalities.

A study also could be conducted to investigate the application of biometrics technology for business registration. Many business owners in Lagos, Nigeria, actually do not have legitimate commercial entities. Biometrics technology can be used to register a business, in which the owner or official of the entity is identified through fingerprint. In

such a case, if the business is involved in suspicious transactions (Internet cafes), the company's personnel will be easily identified based on biometrics data obtained during the business registration exercise.

The banking sector is a prime segment for another type of investigation. The forgery of banking documents is a common occurrence. If a thorough study of this problem is carried out, the results will provide insight into banking management and the need for a reliable mechanism for the identification of bank customers. It will also help to prevent customers' assets from being fraudulently compromised.

Future research might also focus on health concerns. In the literature review, the health concern was a major source of apprehension in developed countries (Bocozk, Buster, Fitzgerald III, Vacca, Welsh, & Wulf, 2005). While there was indication of a similar concern from this study during the interview process, it would be necessary to conduct research that investigates adults' perception about health issues related to biometrics technology adoption.

In addition, a study could be conducted using a similar instrument that changes the research approach of the study. While the current investigation was conducted using mixed methodology, a quantitative approach could be employed to determine the outcome of factors that will influence adults' behavior toward the adoption of biometrics technology. Or, qualitative research method could also be used instead of quantitative approach. Either of these methodologies presents an opportunity to further this study and determine the outcome.

Finally, there are several topics related to implementation and usability that an astute researcher may wish to explore. Such an effort could focus on influences of technical dynamics versus the behaviors and interests of adults when considering biometric security systems. Such an investigation might uncover surprising results between perceptions and particular types of biometrics modalities. The researcher's reflection about the study is presented in the following section.

Reflection

The achievement of completing this investigation epitomizes a triumph due to the challenges the researcher faced. The successful completion of the requirements for a doctoral degree is a significant milestone personally and professionally. From a personal standpoint, it shows determination and level of commitment to invest time and improve skills that will provide an opportunity for advancement and minimize future and long-term unemployment risks. The accomplishment of a doctoral degree requires a high degree of tolerance, dedication, and persistence. The researcher is emboldened after the attainment of this highly coveted and scholarly degree. Professionally, the achievement will place the researcher among educational elites recognized for their astute expertise in their field. A doctorate epitomizes scholarly excellence and this researcher will belong to this class of professionals, subject matter experts, and scholarly elites.

The method of deciding on the research topic, the research instrument, the problem statement, and where to conduct the study was challenging. However, the researcher's professional experience and capabilities in the information technology (IT)

industry both as an instructor with over a decade of in-class room teaching experience and as an analyst proved very helpful. As an IT professional, the researcher has a passion for biometrics technology because of an increasing concern for security both within the society, government, nations, and in industries.

Security is a big concern and the role of biometrics technology for the reliable identification and authentication of individuals is greater than ever. There are everyday discussions, news, and journal articles about identity fraud, terrorist threats, and security apprehensions. An interesting aspect of the investigation was the researcher's decision to focus it on a developing country, Nigeria. Due to the fact that no such study has been carried out in Nigeria, there were considerable challenges and opportunities. It was very difficult to obtain literature and data about Africa and Nigeria. This was very challenging.

The review of the literature revealed that while there are many studies carried out in developed countries, no such investigation has been conducted in Nigeria, in particular, and in Africa, in general, regarding the dynamics that will influence the adoption and implementation of biometrics technology for the mitigation of identity deception. One relevant study was conducted in South Africa by Giesing (2003) on "User perceptions related to identification through biometrics within electronics business." This provided the researcher a researchable topic and offered an opportunity to explore gaps in the literature, which are presented after this section.

The selection of a sampling was not very difficult as many participants were interested and familiar with the technology. They expressed enthusiasm at the capability

of the technique to reliably identify individuals. They were aware of the escalating trend of forgeries and the consequences that result from the problem. The solicitation of participants started with a professional contact who provided other people based on the network of individuals who were capable of participating in the study. The majority of the research subjects saw the effort as a way to express their views about the effects of identity fraud and to support a control measure that will be reliable and effective.

While the researcher personally suspected that biometrics technology would provide positive social impacts as a result of credentialing identity and controlling fraud, the results of this study proved that the dynamics of ease of use, perceived usefulness, security concern, and awareness hindered the adoption and widespread usability of the technology. The findings were surprising to the researcher. For instance, the result of ease of use was 67%. The researcher expected the result to be 52% or less. The result for perceived usefulness was 70% and the investigator expected about 55%. About security concern, it was 42% though the researcher expected this to be 65%. For awareness, the result was 66% but the researcher expected the result to be 50%. These results were significant since each was more than 50% except security concern. Overall, this journey has been an impressive and exciting experience despite the obstacles and challenges encountered in the process. In the next section, the gaps in the literature review for this study are presented.

Gaps in the Literature about the Dynamics of Biometrics Technology Implementation

The literature on biometrics technology indicated the popularity of mainstream biometrics technologies such as fingerprint technique and iris scan in advanced countries (ANSI, 2005; Archarge, 2005; Baird, 2002; Lease, 2005; Mordini & Petrini, 2007). However, for developing nations such as Nigeria, this author found it surprising that there was no literature regarding this technology and its relationship to various dynamics that affected its adoption and implementation. Consequently, the technology acceptance model (TAM) was augmented and provided the account for the proposal and this study. Currently, there are increasing numbers of biometrics system implementations and the concentrations are in Europe and the United States (European Commission, 2005; U. S. Treasury, 2005).

Despite several social, political, economic, and environmental differences between developed and emerging countries, these mainstream biometrics technologies: fingerprint, face, iris, hand, and voice will function properly in developing nations like Nigeria provided that implementations are made according to application and vendors' requirements. The dynamics of influence and adults' willingness to use such technology should also be considered. It is important that biometrics technology vendors, organizations, government and its agencies, as well as individuals become familiar with the factors that will influence the adoption of biometrics technology and usability. This is very important from the researcher's point of view.

The researcher expects that the results of this study will provide a roadmap for other investigations to be carried out that will make meaningful research data available for further scholarly work in developing countries on the African continent. While the gap in the literature posed a difficulty regarding understanding the factors that will influence the adoption of biometrics technology and gauging adults' behaviors toward biometrics systems in emerging nations, the researcher hopes that this study has shed light on this area.

Concluding Statement

Based on the findings and conclusion of this research, the take home message is that ease of use, perceived usefulness, security concern, and awareness are among the dynamics that will influence adults' behavior toward the adoption and usability of biometrics technology. Prior to this investigation, these factors have not been explored with regard to the implementation of biometrics technology in a developing country such as Nigeria. Biometrics technology is increasingly used as a mechanism for determining the identification and credentialing of individuals.

The role of biometrics security systems in accomplishing reliable authentication and the control of identity fraud has been documented in the literature. It has been described as being very critical in the fight against crimes, protection of the border, and in the global war on terrorism (GWOT). Biometrics technology is regarded as a critical component in the next frontier of security and the control of identity fraud, identification, authentication, authorization, and accountability (IA^3) in information technology

industries, businesses, government and its agencies, and among individuals. This had made its widespread implementation, application, and usability paramount both in developed nations and emerging countries.

As discussed in chapter 2, numerous researchers have recognized the security benefits of biometrics technology (Brobeck & Folkman, 2005; Giarimi & Magnusson, 2002; Ngugi, 2005; Sherwood, 2008; TRUSTe, 2005). The literature review revealed that biometrics technique appears to be the most popular method of authentication, in general, with the majority of research participants in developed countries agreeing that they would prefer to use biometrics technology to verify their identity as opposed to tokens or passwords (Jones, Anton, & Earp, 2007; King, Lee, Turban, & Viehland, 2004; LogicaCMG, 2006). A similar finding was confirmed in this investigation.

Many national governments, organizations, and businesses, as well as individuals, have recognized the benefits of biometrics security systems. However, many scholars, experts, and advocacy groups such as Electronic Frontier Foundation have noted concerns about privacy (Bocozk, Buster, Fitzgerald III, Vacca, Welsh, & Wulf, 2005). However, the apprehensions around privacy issues do not deter increasing implementation and application in developed countries. As many surveillance systems seek to locate and track individuals, biometrics systems present the greatest danger precisely because of the promise of extremely high accuracy (Electronic Frontier Foundation, 2007). Such extreme reliability is very important for function-effectiveness in identity verification.

Though biometrics technology is changing the landscape of the security industry in developed countries, the findings of this study indicated that many developing nations have not implemented such a technique for reasons beyond the scope of this investigation. Nevertheless, as identity fraud continues to be noted as both a national and global problem, the results of this study will provide a justifiable rationale for the adoption and usability of this technology in a developing country such as Nigeria. Biometrics vendors have the opportunity to explore the findings of this study and capitalize on them with regard to the dynamics uncovered in this investigation and relative to particular biometrics technology.

For this study, the researcher expects that the result could be beneficial to other scholars, businesses, biometrics vendors, individuals, professionals, educators, organizations, government and its agencies, and security industries. Therefore, the government, stakeholders, and biometrics vendors should develop and maintain partnerships to promote the awareness, adoption, and usability of biometrics technology for the control of crimes and to preserve the data of individuals for reliable identification, authentication, authorization, and accountability.

References

Abernathy, W., Lien, T., and Granger, S. (2006). Biometrics: Who's watching you? *Electronic Frontier Foundation.* Retrieved from http://www.eff.org/Privacy/Surveillance/biometrics/

Acharya, L. (2006). *Biometrics and government*. Parliamentary Information and Research Service. Retrieved from http://www.parl.gc.ca/information/library/PRBpubs/prb0630-e.pdf

AlBalawi, W. (2006). *Students'and instructors' attitudes toward using biometric technology as an identification method in online courses*. (Unpublished doctoral dissertation). West Virginia University, Morgantown.

Allan, A. (2002). *Biometrics: How do they measure up?* Stamford, CT: Gartner Research.

Allan, A. (2006). *Biometric authentication: Perspective.* Stamford, CT: Gartner Research.

Alrafi, A. (2005). *Technology acceptance model*. Retrieved from http://www.leedsmet.ac.uk/inn/RIP2005-4.pdf

American National Standards Institute. (2007). *Cross-jurisdictional and societal aspects of implementation of biometric technologies, Part 1: Guide to the accessibility, privacy, and health and safety issues in the deployment of biometric systems for commercial applications*. New York: International Standard Organization.

Anaf, S. & Sheppard, L. A. (2007). Mixing research methods in health professional

degrees: Thoughts for undergraduate students and supervisors. *The Qualitative Report*, *12*(2), 184–192.

Anonymous. (2004). U.S. starts fingerprint program. *Cable News Network.* Retrieved from http://www.cnn.com/2004/US/01/05/fingerprint.program/index.html

Anonymous. (2006). Biometrics frequently asked questions. *National Science and Technology Council*. Retrieved from http://www.biometrics.gov/Documents/FAQ.pdf

Anonymous. (2007a, June 9). Fraud ring uncovered in Nigeria. *British Broadcasting Corporation.* Retrieved from http://news.bbc.co.uk/2/hi/africa/6982375.stm

Anonymous. (2007b). *What is database? A word definition from the Webopedia Computer*. Retrieved from http://www.webopedia.com/TERM/D/database.html

Anonymous. (2009). *Lagos State Government: Investment potentials*. Retrieved from http://www.lagosstate.gov.ng/index.php?page=subpage&spid=16&mnu=null

Answers Corporation. (2009). *Task.* Retrieved from http://www.answers.com/topic/task

Argus Solutions. (2007). *Iris recognition: How it works*. Retrieved from http://www.argus-solutions.com/how_iris_recognition_works.htm

Asfaw, M. (2006). *Sociopersonal Factors Affecting the Adaptation and Use of Information and Communication Technologies Within Ethiopia.* Retrieved from Business Source Premier database.

AuthenTec, (2008). AuthenTec: Survey shows highly favorable consumer perceptions for

fingerprint sensors. *Computer, Networks, & Communications*.

Ayantokun, O. (2006, June 8). Fighting cyber crime in Nigeria. *InfoSec News.* Retrieved from http://www.infosecnews.org/hypermail/0606/11398.html

Baird, S. L. (2002). Biometrics "Security Technology": It is important for students to understand that technology can be used as part of a solution to a problem. *The Technology Teacher, 61*, 1–6.

Ballard, M. (2006, May 22). Biometric whitewash gathers pace. *The Register.* Retrieved from http://www.theregister.co.uk/2006/05/22/biometric_whitewash/print.html

Barry, C. (2002). *Financial institutions give biometrics a thumbs up.* Retrieved from http://www.tmcnet.com/biomag/features/celnet.htm

Bartlett II, J. E, Kotrlik, J. W; and Higgins, C. C. (2001). Organizational research: determining appropriate sample size in survey research. *Information Technology, Learning, and Performance Journal*, Vol. 19, No. 1, Spring, pp. 43–50.

Beekhuyzen, J., Hellens, L., Siedle, M., Topor, R., & Stevens, S. (2004). Health biometrics: Ready to be a smart Internet technology? *Malaysian Journal of Computer Science*, *17*(2), 90–97.

Bick Financial Security Corporation. (2009). *Identity fraud: Protect your personal information*. Ancaster, Ontario, Canada.

Blair, J. (2010). *Pretesting.* Bethesda, MD: Abt Associates.

Blackburn, D. M. (2004). *Biometrics 101*. Washington, DC: Federal Bureau of Investigation, Government Printing Office.

Blackburn, D., Coty, T., Cook, J., Dee, T., & Dunn, J. (2008). *Biometrics in government post-9/11: Advancing science, enhancing operations.* Washington, DC: Office of Science and Technology Policy.

Blackburn, D., Miles, C., & Wing, B. (2006). *The national biometrics challenge*. Washington, DC: National Science and Technology Council Subcommittee on Biometrics, Government Printing Office.

Blackburn, D. & Turner, A. (2002). Biometrics: Separating myth from reality. *Corrections Today, 64*(7), 140–141.

Bocozk, K, Buster, C. J., Fitzgerald III, S., Vacca, E. E., Welsh, J., and Wulf, T. (2005). *Biometrics: Networks and telecommunications in business.* Retrieved from http://www.kevingalls.com/biometrics/groupproject.doc

Brackin, D. (2005, July 1). *News Release: Nigerian man sentenced for identity fraud.* Sherman, Texas: Office of the United States Attorney. Retrieved from http://www.usdoj.gov/usao/txe/news_release/news/akanmu_hagan.pdf

Bragg, R., Ousley, M. R., & Strassberg, K. (2004). *Network security: The complete reference*. Emeryville, CA: McGraw-Hill/Osborne.

Brew, T. (2006). *European attitudes towards biometrics*. Hampstead, London LogicaCMG.

Brobeck, S. & Folkman, T. (2005). *Biometrics–Attitudes and factors influencing a breakthrough in Sweden*. Jonkoping International Business School. Jonkoping, Sweden.

Bromba, M. (2007). *Bioidentification: Frequently asked questions*. Retrieved from http://www.bromba.com/faq/biofaqe.htm

Bruno, M. (2001). Biometrics are too hot to handle: Despite high hopes, bankers are still all talk when it comes to identification technology. *Bank Technology News*, *14*(9), 30–33.

Brydie, D. R. (2008). *Situational considerations in information security: Factors influencing perceived invasiveness toward biometrics.* (Unpublished doctoral dissertation). Capella University, Minneapolis.

Buber, R., Gadner, J., and Richards, L. (2004). Issues in mixing qualitative and quantitative approaches to research. In *Applying qualitative methods to marketing management research* (pp. 141–156). Burber, Gadner, and Richards, UK: Palgrave Macmillan.

Bucci, H. P. (2003). *The value of Likert scales in measuring attitudes of online learners.* Retrieved from http://www.hkadesigns.co.uk/websites/msc/reme/likert.htm

Campbell, L. M. (2005). *Rising government use of biometric technology: An analysis of the United States Visitor and Immigrant Status Indicator Technology Program.* Retrieved from http://www.isrcl.org/Papers/2005/Campbell_L.pdf

Cano, V. (2009). *Foundation Steps: Questionnaire or interview?* Retrieved from http://www.qmu.ac.uk./psych/RTrek/foundation/f10.htm

Caracelli, V. J., & Greene, J. C. (1993, Summer). Data analysis strategies for mixed-method evaluation designs. *Educational Evaluation and Policy Analysis, 15*(2),

195–207.

Caslon Analytics Biometrics. (2006). *Biometrics, attitudes and responses*. Retrieved from http://www.caslon.com.au/biometricsnote12.html

Cassell, E. J. (2000, July–August). The principles of the Belmont Report revisited: How have respect for persons, beneficence, and justice been applied to clinical medicine? *Hastings Center Report, 30*(4), 20–21.

Cavoukian, A. (1999). *Consumer biometric applications: A discussion paper*. Toronto, Ontario, Canada: Information and Privacy Commissioner.

Chaffey, D., Chadwick, F. E., Mayer, R., and Johnson, K. (2006). *Internet marketing: Strategy, implementation, and practice.* New York: Prentice Hall.

Chandra, A. and Calderon, T. G. (2003). Toward a biometric security layer in accounting systems. *Journal of Information Systems, 17*(2), 51–70.

Chandra, A. and Calderon, T. (2005). Challenges and constraints to the diffusion of biometrics in information systems. *Communications of the ACM*, *48*(12), 101–106.

Chirillo, J. and Blaul, S. (2003). *Implementing biometric security*. Indianapolis, IN: Wiley Publishing, Inc.

Choo, K. S., Gordon, G. R., Gordon, J. B., and Rebovich, D. J. (2007). *Identity fraud trends and patterns: Building a data-based foundation for proactive enforcement*. New York: Center for Identity Management and Information Protection, Utica College.

Collins, K. M. T. and Onwuegbuzie, A. J. (2007). A typology of mixed methods sampling designs in social science research. *The Qualitative Report, 12*(2), 281–316.

Coventry, L. (2005). *Usable biometrics offer a technological solution to the authentication of individuals*. Dundee, UK: Advanced Technology & Research, NCR Financial Solutions.

Cowen, J. B. (2009). The influence of perceived usefulness, perceived ease of use, and subjective norm on the use of computed radiography systems: A pilot study. Retrieved from https://kb.osu.edu/dspace/bitstream/1811/36983/1/FinalSubmitted.pdf.

Creative Research Systems (2009). *Survey Design.* Retrieved from www.surveysystem.com/sdesign.htm

Creswell, J. W. (1998). *Qualitative inquiry and research design: Choosing among five traditions*. Thousand Oaks, CA: Sage Publications.

Creswell, J. W. (2003). *Research design: Qualitative, quantitative, and mixed methods approaches* (2nd ed.). Thousand Oaks, CA: Sage Publications.

Crowley, M. G. (2006). *Cyber crime and biometric authentication–The problem of privacy versus protection of business assets*. Perth, Australia: School of Law and Justice, Edith Cowan University.

Daugman, J. (1993). High confidence visual recognition of persons by a test of statistical

independence. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, *15*(11), 1148–1161.

Davis, F. D. (1993). User acceptance of information technology: System characteristics, user perceptions and behavioral impacts. *International Journal of Machine Studies*, *38*, 475–487.

Davis F. D. (2001). *Perceived usefulness, perceived ease of use, and user acceptance of information technology.* Ann Arbor: Computer and Information Systems, Graduate School of Business Administration, University of Michigan.

Davis, S. G. (1994). Touching Big Brother: How biometric technology will fuse flesh and machine. *Information Technology & People, 7*(4), 1–9.

DeMaio, T. J., Rothgeb, J., & Hess, J. (1998). *Improving survey quality through pretesting*. Washington, DC: U. S. Bureau of the Census.

Deschaine, D. A. (2005). *An analysis of biometric technology as an enabler to information assurance*. (Unpublished master's thesis). Air Force Institute of Technology, Wright-Patterson Air Force Base, Columbus, Ohio.

Dixon, N., Giskes, R., & Sampford, K. (2005). *Identity fraud*. Retrieved from http://www.parliament.qld.gov.au/view/publications/documents/research/ResearchBriefs/2005/200503.pdf

Dominic, A. C. (2007). *Access to knowledge created by information technology vendors and client staff work performance.* Retrieved from Business Source Premier database.

Dror, I. (2006). A holistic–cognitive approach for success. *Biometric Technology Today*, *14*(7–8), 7–8.

Dyke, J. V. (2009). Research shows identity fraud affecting nearly ten million Americans. *Javelin Strategy and Research.* Retrieved from http://www.javelinstrategy.com/2009/02/09/latest-javelin-research-shows-identity-fraud-in....

Electronic Frontier Foundation. (2006). Biometrics: Who's watching you? *Electronic Frontier Foundation.* Retrieved from http://www.eff.org/wp/biometrics-whos-watching-you

Elliot, S. J., Massie, S. A., & Sutton, M. J. (2007). The perception of biometric technology: A survey. *IEEE*, *7*(8), 259–264.

Ernst, J. (2002). *The iris recognition homepage: Iris recognition and identification*. Retrieved from http://www.iris-recognition.org/

European Commission. (2005). *Biometrics at the frontiers: Assessing the impact on society*. Spain: Joint Research Center, Institute of Prospective Technological Studies, Seville, pp. 1–166.

Faulkner, P. (2005). *Consumer acceptance of biometric technology within the UK National ID Card Scheme*. Portsmouth, UK: Portsmouth Business School.

Fenn, J. (1999). *Case study: Fingerprint verification for network security*. Stamford, CT: Gartner Research.

Fingerprint Technology. (2006, March 27). Fingerprint technology LTD integrates 123ID

matching in Nigerian national pension program. *Find Biometrics: Global Identity Management.* Retrieved from http://www.findbiometrics.com/viewnews.php?id=3104

Gall, M. D., Gall, J. P., and Bong, W. R. (2003). *Educational Research: An introduction*, (7^{th} ed.). Boston: Pearson Education.

Garcia, J. R. G., and Pardo, T. A. (2006). Multi-method approaches to digital government research: Value lessons and implementation challenges. *Proceedings of the 39th International Conference on System Sciences, Vol. 4* (1–11). Hawaii.

Gaudin, S. (2003). *Poll: Biometrics gaining acceptance*. Retrieved from http://www.esecurityplanet.com/trends/print.php/1566401

Giarimi, S. and Magnusson, H. (2002). *Investigation of user acceptance for biometric verification/identification methods in mobile units*. (Unpublished master's thesis). Department of Computer and Systems Sciences, Stockholm University/Royal Institute of Technology, Stockholm.

Gideon, F. (2002). U.S. warns Nigeria over online fraud schemes. *Computer Crime Research Center.* Retrieved from http://www.crime-research.org/news/2002/09/Mess2801.htm

Giesing, I. (2003). *User perceptions related to identification through biometrics within electronic business*. (Unpublished master's thesis). Commerci, Department of Informatics, University of Pretoria, South Africa.

Global Aging. (2008, February 28). *Global action on aging: Rural poverty in Nigeria*.

Retrieved from http://www.globalaging.org/ruralaging/world/2008/nigeria.htm

Global Security. (2009). *Homeland security: Fingerprint identification systems*. Retrieved from http://www.globalsecurity.org/security/systems/biometrics-fingerprint.htm

Gordon, G. R., and Willox, N. A. (2003). *Identity fraud: A critical national and global threat.* New York: Economic Crime Institute, Utica College.

Gordon, G. R., and Willox, N. A. (2006). *The ongoing critical threats created by identity fraud*. New York: Economic Crime Institute, Utica College.

Gregorio, S. D. (2000). *Using NVIVO for your literature review.* London: Institute of Education.

Grijpink, J. (2005). Biometrics and identity fraud protection: Two barriers to realizing the benefits of biometrics–A chain perspective on biometrics and identity fraud–Part II. *Computer Law & Security Report*, *21*(3), 249–256.

Hampe, J. F., Krulle, G. R., and Rebne, D. S. (2005). *Biometrics and e-identity (e-passport) in the European Union: Overcoming POC-cultural diversity for common cause?* Landau, Germany: University of Koblenz.

Hanson, W. E., Plano Clark, V. L., Petska, K. S., Creswell, J. W., and Creswell, J. D. (2005). Mixed methods research designs in counseling psychology. *Journal of Counseling Psychology, 52*(2), 224–235.

Harris, A. J. and Yen, D. C. (2002). Biometric authentication: Assuring access to information. *Information Management & Computer Security, 10*(1), 12–19.

Harris, K. (1999). *Biometrics: An ATM identification replacement?* Stamford, CT: Gartner Research.

Harrison, A. (2002). *Researcher: Biometrics unproven, hard to test.* Retrieved from http://www.securityfocus.com/news/566

Heckle, R. R., Patrick, A. S., and Ozok, A. (2007 July). Perception and acceptance of fingerprint biometric technology. *Symposium on Usable Privacy and Security (SOUPS),* Pittsburgh, PA, USA, pp. 1–2.

Heyer, R. (2008). *Biometrics technology review 2008.* South Australia, Edinburgh, *Defense science and technology Organization.*

Hing, L., Jain, A. K., Pankanti, S., Prabhakar, S., Ross, A., & Wayman, J. L. (2004, August). Biometrics: A grand challenge. *The Proceedings of the International Conference on Pattern Recognition*, Cambridge, UK.

Holetzky, S. (2009). What is GWOT? *Wise Geek.* Retrieved from http://www.wisegeek.com/what-is-gwot.htm

Hong, J. H., Yun, E. K., & Cho, S. B. (2005). A review of performance evaluation for biometrics systems. *International Journal of Image and Graphics, 5*(3), 501–536.

Hsieh, C., Nguyen, Y., and Lin, B. (2008). *Implementation of biometrics payment technology in organizations*. Retrieved from http://www.decisionsciences.org/Proceedings/DSI2008/docs/106-7315.pdf

Hulse, S. F. (2009). *Instructional techniques: Test statistics.* Retrieved

from https://www.asrt.org/Media/Pdf/ForEducators/4_InstructionalTechniques/4.11TestStats.pdf

Hunt, S. D., Sparkman Jr., R. D., & Wilcox, J. B. (1982, May). The pretest in survey research: Issues and preliminary findings. *Journal of Marketing Research*, *19*(2), 269–273.

International Biometric Group. (2006). *Biometric market by technology, 2007*. Retrieved from http://www.biomertricgroup.com/reports/public/market_report.php

International Biometric Group. (2007). *The biometric industry: One year after 9/11*. Retrieved from http://www.ibgweb.com/9-11.html

International Biometric Group. (2008). *Independent biometrics enterprise*. Retrieved from http://www.biometricgroup.com/reports/public/market_report.html

International Development Research Center (IDRC) (2011). *Module 7: Disseminating research findings.* Retrieved from http://www.idrc.ca/en/ev-106565-201-1-DO_TOPIC.html

Investopedia (2010). *Descriptive statistics*. Retrieved from http://www.investopedia.com/terms/d/descriptive_statistics.asp

Jackson, C. (2008). *Global study finds majorities of online consumers are concerned about identity theft and fraud*. New York: Ipsos Public Affairs.

Jahangir, N; Begum, N. (2008). The role of perceived usefulness, perceived ease of use,

Security and privacy, and customer attitude to engender customer adaptation in the context of electronic banking. *African Journal of Business Management,* Vol. 2, pp. 032–040.

Jain, A., Bolle, R., & Pankanti, S. (n.d). *Introduction to biometrics*. East Lansing: University of Michigan.

Jain, A. K., and Ross, A. (2004). Multibiometric systems. *Communications of the ACM*, *47*(1), 34–40.

Jain, A. K., and Ross, A. (2008). *Biometrics recognition: Techniques, applications and challenges*. Retrieved from http://www.comp.hkbu.edu.hk/~icpr06/tutorials/Jain.html

Jain, A. K., Ross, A. and Prabhakar, S. (2004). An introduction to biometric recognition. *IEEE*, *14*(1), 1–29.

Jamieson, R., Stephens, G. and Kumar, S. (2005). Fingerprint identification: An aid to the authentication process. *Information Systems Control Journal, 1*, 1–4.

Johnson, B. R., and Onwuegbuzie, A. J. (2004). Mixed methods: A research paradigm whose time has come. *Educational Researcher*, *33*(7), 14–26.

Johnson, H. (2006). *Mixed research: Mixed method and mixed model research*. Retrieved from http://www.Southalabama.edu/coe/bset/johnson/lec14.htm

Jones, L. A., Anton, A. I., and Earp, J. B. (2007). *Towards understanding user perceptions of authentication technologies*. Alexandria, VA: WPES.

Joppe, M. (2000). *The research process*. Retrieved from

http://www.ryerson.ca/~mjoppe/rp.htm

Joshua, A. J., and Koshy, M. P. (2009). Attitudes and behavioural intentions towards a technology based self-service banking delivery channel: The case of ATMs. *Erudition, The Albertian Journal of Management,* 81–94.

Khaw, P. (2002). *Iris Recognition Technology for Improved Authentication.* Silver Spring, MD: SANS Institute.

Kim, J. (2006). *Biometrics in hotel industry: Issues that impact customers' acceptance.* (Unpublished master's thesis). University of Las Vegas, Las Vegas, Nevada.

Kim, J. S., Brewer, P., and Bernhard, (2008). Hotel customer perceptions of biometric door locks: Convenience and security factors. *Journal of Hospitality Marketing & Management*, *17*(1), 162–183.

King, D., Lee, J., McKay, J., Marshall, P., Turban E., and Viehland, D. (2008). *A managerial perspective*. Upper Saddle River, NJ: Prentice Hall Inc.

King, D., Lee, J., Turban, E., and Viehland, D. (2004). *Electronic commerce: A managerial perspective*. Upper Saddle River, NJ: Prentice Hall Inc.

Klopping, I. M., and McKinney, E. L. (2004). Extending the technology acceptance model and the task-technology fit model to consumer e-commerce. *Information Technology, Learning, and Performance Journal, 22*(1), 35–48.

Kristin, D., and Erin, B. (2001). Anatomy of fraud. *Kiplinger's Personal Finance*, *55*(3), 88–96.

Kumar, V., Kuma, U., Lavassani, K. and Movahedi, B. (2007). *Measures of identity*

fraud. Ottawa, Ontario, Canada: Sprott Research Program, Carleton University.

Lanitis, A. (2009). *Facial biometric templates and aging: Problems and challenges for artificial intelligence.* Lemesos, Cyprus: Cyprus University of Technology.

Lawrence, S. (2005). Biometrics bring fingerprint ID to hospitals. *CIO Insight.* Retrieved from http://www.cioinsight.com/print_article2/0,1217,a=148427,00.asp

Lease, D. R. (2005). *Factors influencing the adoption of biometric security technologies by decision making information technology and security managers.* (Unpublished doctoral dissertation). Capella University, Minneapolis.

Leedy, P. A., & Ormrod, J. E. (2001). *Practical research: Planning and design* (7th ed.). Columbus, OH: Merrill Prentice-Hall.

Lewis, M. (2007). *Biometrics demystified white paper*. London: Information Risk Management, Kings Building Square.

Liu, S., Silverman, M. (2001, January/February). A practical guide to biometric security technology. *IT Pro*, 27–32.

Liu, Y. (2008). Identifying legal concerns in the biometric context. *Journal of International Commercial Law and Technology, 3*(1), 45–54.

LogicaCMG. (2006). *e-Identity: European attitudes towards biometrics*. Hampstead, London: Vanson Bourne.

Mahinda, E., and Whitworth, B., (2005). The web of system performance: Extending the TAM model. *Information Systems Evaluation Track.* Americas Conference on Information Systems, Omaha, Nebraska, USA, 367–374.

Malhorta, Y., and Galletta, D. F. (1999). Extending the technology acceptance model to account for social influence: Theoretical bases and empirical validation. *Proceedings of the 32nd International Conference on System Science, Vol. 1*, *Hawaii, USA, pp. 1-14.*

Mansfield, T. (2009). *Biometric authentication in the real world.* Middlesex, United Kingdom: Centre for Mathematics and Scientific Computing National Physical Laboratory.

Marburger, III, J. H. (2008). *Biometrics in government post-9/11*. Washington, DC: Government Printing Office.

Markowitz, J. A. (2000). Voice biometrics. *Communications of the ACM*, *43*(9), 66–73.

Markowitz, J. and Gravell, W. (2007). *Report of the Defense Science Board Task Force on defense biometrics*. Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, Government Printing Office, Washington, DC.

Matters, T. (2003). *Family and community services research news,* (17), pp. 1–8.

Matyas, V. and Riha, Z. (n.d). *Biometric authentication—Security and usability.* Retrieved from http://www.fi.muni.cz/usr/matyas/cms_matyas_riha_biometrics.pdf

Maxim, P. (1999). *Quantitative research in the social sciences.* New York: Oxford University Press, Inc.

Mordini, E., and Petrini, C. (2007). Ethical and social implications of biometric

identification technology. *Ann Ist Super Santa*, *43*(1), 5–11.

Morgan, D., and Krouse, W. (2005). Biometric identifiers and border security: 9/11 Commission recommendations and related issues. *Congressional Research Service,* Washington, DC.

Murph, D. (2007, September 13). Panasonic develops walkthrough iris scanner to hasten ID checks. *Engadget.* Retrieved from http://www.engadget.com/2007/08/13/

Nakashima, E. (2007, December 22). FBI prepares vast database of biometrics. *The Washington Post,* p. A01.

Narins, P. (1999). *Get better info from all your questionnaires: 13 important tips to help you pretest your surveys.* Retrieved from http://www.htm.uoguelph.ca/MJResearch/ResearchProcess/PretestingTips.htm

National Science Technology Council (NSTC). (2006a). *Biometrics glossary: Introduction*. Washington, DC: Government Printing Office.

National Science Technology Council. (2006b). *The national biometrics challenge*. Washington, DC: Government Printing Office.

National Science Technology Council. (2006c). *Subcommittee on biometrics and identity management committee on technology*. Washington, DC: Government Printing Office.

National Science Technology Council. (2006d). *Privacy and biometrics: Building a conceptual foundation*. Washington, DC: Government Printing Office.

National Science Technology Council. (2006e). *Fingerprint recognition.* Washington, DC: Government Printing Office.

Newman, G. R., and McNally, M. M. (2005). *Identity theft literature review*. Washington, DC: National Institute of Justice, Office of Justice Programs, U.S. Department of Justice, Rutgers University, Newark.

Newton, E. M., and Woodward, J. D. (2001). *Biometrics: A technical primer*. Santa Monica, CA: Rand Corporation.

Ngugi, B. (2005). *Electronic capture and analysis of fraudulent behavioral patterns: An application to identity fraud.* (Doctoral dissertation). New Jersey Institute of Technology, Newark, New Jersey.

Norman, W. A., Jr., and Thomas, R. (2005). Unmasking terrorist identity fraud. *USA Today Magazine, 134*(2724), 24–26.

Norris, P. (2001). *Digital divide: Civic engagement, information poverty and the Internet in domestic societies.* New York: Cambridge University Press.

Nyasulu, J. & Fomene, T. (2001). *Report on the literature of iris biometric technology*. Linkopings University, Linkoppings, Sweden.

O' Connor, T. (2006). *Data analysis.* Retrieved from http://www.apsu.edu/oconnort/3760/3760lect07.htm

Oghre, B. (2007). Nigeria must have a biometric citizen database. *Nigeria Matters.* Retrieved from http://www.nigeriansinamerica.com/articles/2075/1/Nigeria-MUST-Have-A-Biometric-Citizen-Database/Page1.html

Onwuegbuzie, A. J., & Leech, N. L. (2006). Linking research questions to mixed methods data analysis procedures. *The Qualitative Report*, 11(3), 474–498.

Opinion Research Corporation (ORC). (2002). *Public attitudes toward the use of biometric identification technologies by government and private sector*. Princeton, New Jersey: Opinion Research Corporation.

Parnaby, P. (2007). *Evaluation through surveys: Collecting and analyzing data is easier with technological tools.* Retrieved from http://www.idea.org/page102.html

Perl, R. (2003). *Terrorism, the future, and U.S. foreign policy*. Retrieved from http://www.fas.org/irp/crs/IB95112.pdf

Pilgrim, T. (2007, November 21). *Biometrics and privacy.* Retrieved from http://www.privacy.gov.au/materials/types/speeches/view/6324

Ploeg, I. V. D. (2005*). Biometric Identification Technologies: Ethical Implications of the Informatization of the Body. BITE Policy Paper no.1,* Retrieved from http://www.biteproject.org/documents/policy_paper_1_july_version.pdf

Podder, B. (2005). *Factors influencing the adoption of Internet banking: A New Zealand perspective.* (Unpublished master's thesis). Auckland University of Technology, Auckland, New Zealand.

Presser, S. & Blair, J. (1994). Survey pretesting: Do different methods produce different results? *Sociology Methodology, 24*, 73–104.

Questbiometrics. (2005). *Advantages of biometrics: Why opt for biometric technology?*

Retrieved from http://www.questbiometrics.com/advantages-of-biometrics.html

Radack, S. (2009). *Biometrics technologies: Helping to protect information and automated transactions in information technology systems*. Retrieved from http://www.itl.nist.gov/lab/bulletns/bltnsep05.htm

Rajchel, L. (2007). *Cross-jurisdictional and societal aspects of implementation of biometric technologies, part 1: Guide to the accessibility, privacy, and health and safety issues in the deployment of biometric systems for commercial applications*, New York: International Standard Organization.

Rand, (2001). *Army biometric applications: Identifying and addressing sociocultural concerns.* Santa Monica, CA: Rand Publications.

Rao, A. S. (n.d.). *Technology acceptance model for complex technologies in a period of rapid catching-up*. Bhawan, New Delhi, India: Department of Scientific and Industrial Research, Technology.

RaviRaj Technologies. (2007). *Biometrics fingerprint technology*. Retrieved from http://www.ravirajtech.com/biometrics_fingerprint_technology.html

Reedman, C. (2004). *UK biometrics and related technologies 2004: New directions in innovation and exploitation*. London: Department of Trade and Industry.

Riley, A. R., and Kleist, F. (2005). The biometrics technologies business case: a systematic approach. *Information Management & Computer Security, 13*, 89–105.

Rocco, T. S., Bliss, L. A., Gallagher, S., and Prado, A. P. (2003). Taking the next step: Mixed methods research in organizational systems. *Information Technology,*

Learning and Performance Journal, 21(1), 19–29.

Roethenbaugh, G. (1997). *Biometrics explained*. Washington, DC: International Committee for Information Technology Standards.

Rosenzweig, P., Kochems, A., and Schwartz, A. (2004 June 21). Biometrics technologies: Security, legal, and policy implications. *Legal Memorandum*, The Heritage Foundation, No. 12, pp. 1–10.

Ross, A. A. (2003). *Information fusion in fingerprint authentication*. (Unpublished doctoral dissertation). Michigan State University, East Lansing.

Ruggles, T. (2002, August 19). *Biometric technical assessment*. Retrieved from http://www.bioconsulting.com/Bio_Tech_Assessment.html

Sale, J. E. M., Lohfeld, L. H., and Brazil, K. (2002). Revisiting the quantitative-qualitative debate: Implications for mixed methods research. *Quality & Quantity*, *36*, 43–53.

SANS. (2002a). *Biometric technology stomps identity theft*. Silver Spring, MD: SANS Institute.

Sasse, A. M. (n.d). *Usability and user acceptance of biometrics*. London: University College.

Savastano, I. M. and Riccardi, L. (2005). *Technical and non-technical problems in biometric physical access control systems.* Institute of Biostructure and Bioimages, National Research Council of Italy, University of Napoli, Italy.

Securityfocus. (2009, February 11). *Survey: Identity fraud climbs, but costs less*.

Retrieved from http://www.securityfocus.com/brief/907

Seyal, A. H., and Tajuddin, S. T. HJ. (n.d.). *A study of Bruneian executives' attitudes on biometrics: An application of theory of reasoned action*. Department of Computing & Information Systems, Institute of Technology, Brunei Darussalam.

Shafir, M. (2006). *Traceless biometric technology: Enabling secure transactions without storage of unique biometric information.* Retrieved from http://www.innovya.com/Innovya_Traceless_biometrics-Michael_(Micha)_Shafir.pdf

Shanks, Tansley, and Weber (2003). Using ontology to validate conceptual models. *Communications of the ACM*, *46(10)*, 85–89. Retrieved from Business Source Premier database.

Shen, D., Laffer, J., Lin, Yimei, and Huang, Xinxin. (2006, Winter). Social influence for perceived usefulness and ease-of-use of course delivery systems. *Journal of Interactive Online Learning, 5*(3), 270–282.

Sherwood, J. (2008, September 29). IT bosses eye up biometric security. *VNUNET.* Retrieved from http://www.infomaticsonline.co.uk/vnunet/news/2125939/bosses-eye-biometric-security

Short, B. (2002). *Getting the 411 on biometrics. Security*. Retrieved from Business Source Premier database.

Silverman, D. (1997). *Qualitative research: Theory, method, and practice*. Thousand

Oaks, CA: Sage Publications, Inc.

Singleton, R., and Straits, B. (2005). *Approaches to social research* (4th ed.). New York: Oxford University Press.

Slover, E. M. (2007). *A case study: Why commercial health and fitness facilities achieve defined key performance indicators.* (Unpublished doctoral dissertation). University of Phoenix, Arizona.

Smith, A. (2002). *Identity fraud report*. Whitehall, London: Economic and Domestic Secretariat, Cabinet Office.

Smith, R. G. (2005, November 21). Biometric solutions to identity-related crime: Evidence versus policy. *Australian Institute of Criminology*, Sydney, Australia, pp. 1–11.

Smith, R. G., Holmes, M. N., and Kaufmann, P. (1999). Nigerian advance fee fraud. *Australian Institute of Criminology trends & issues in crime and criminal justice,* No. 121, Canberra, Australia, pp. 1–6.

Sollie, R. S. (2005). *Security and usability assessment of several authentication technologies.* (Unpublished master's thesis). Department of Computer Science and Media Technology, Gjovik University College, Gjovik, Norway.

Stana, R. M. (2002). *Identity fraud: Prevalence and links to alien illegal activities.* Washington, DC: Government Accounting Office.

Stempel, J. (2009). US '08 identity fraud up in dollars, victims. *Reuters.* Retrieved from http://www.reuters.com.article/bondsNews/idUSN0646389320090209

Stephen, C. (2000). Biometrics: Solving cases of mistaken identity and more. *FBI Law Enforcement*, *69*(6), 9–16.

Sukhai, N. B. (2004). *Access control and biometrics.* Retrieved from http://www.utc.edu/Faculty/Li-Yang/CPSC415/access-control-biometrics-p124-sukhai.pdf

Taneja, A., Wang, A., and Reja, M. K. (n.d). *Assessing the impact of concern for privacy and innovation characteristics in the adoption of biometrics technologies*. University of Texas at Arlington, TX, pp. 133-141.

Tashakkori, A. and Teddlie, C. (1998). *Mixed methodology: Combining qualitative and quantitative approaches.* Thousand Oaks, CA: Sage Publications.

Tierney, J. (2001, November 20). The Big City; For air safety, an E-Z pass using retinas. *The New York Times.* Retrieved from http://query.nytimes.com/gst/fullpage.html?res=9D04E0DC1E3BF933A15752C1A9679C8B63&sec=&spon=&pagewanted=print

Tilton, C. J. (2006). *The role of biometrics in enterprise security*. Retrieved from http://www.dell.com/downloads/global/powers/ps1q06-20050132-Tilton-OE.pdf

Tiresias, O. (2008). *An introduction to biometrics*. Retrieved from http://www.tiresias.org/research/guidelines/biometrics.htm

Towers Group. (2001). Study sees slow acceptance of biometrics technologies. *Credit Union Journal, 5*(49), 1.

Townsend, M. (2009). *Four million Britons have fallen victim to identity fraud.* Retrieved

from http//www.managingrisc.com/default

Transportation Security Administration. (2008). *TSA registered traveler: Security, privacy and compliance standards for sponsoring entities and service providers, version 3.1.* Retrieved from http://www.tsa.gov/assets/pdf/rt_standards_v3.1.pdf

Trochim, W. M. K. (2006). *Descriptive statistics: Research methods knowledge base.* Retrieved from http://www.socialresearchmethods.net/kb/statdesc.php

Trochim, W. M. K. (2006). Descriptive Statistics: Research Methods Knowledge Base. Retrieved from http://www.socialresearchmethods.net/kb/statinf.php

TRUSTe. (2005). *Consumer attitudes about biometrics in ID documents*. Retrieved from https://www.truste.org/pdf/Biometrics_study.pdf

Unisys. (2005). *Unisys 2005 identity fraud global consumer report*. Unisys Corporation, Blue Bell, PA.

Unisys. (2006, May 3). *Consumers worldwide support biometrics for IDs*. Retrieved from http://www.scoop.co.nz/stories/print.html?path=SC0605/S00013.htm

United Nations Cyberschoolbus. (2009). *Lagos, Nigeria*. Retrieved from http://www.un.org/cyberschoolbus/habitat/profiles/lagos.asp

United States Treasury. (2005). The use of technology to combat identity theft. *Report on the Study Conducted Pursuant to Section 157 of the Fair and Accurate Credit Transactions Act of 2003.* Washington, DC: General Accounting Office.

University of North Carolina. (2009). *Literature reviews*. Retrieved from

http://www.unc.edu/depts/wcweb/handouts/literature_review.html

Vance, C. (October 11, 2002). *Biometrics*. Retrieved from http://www.bufuinc.com/library/articles/Vance-tsm340-Biometrics.doc

Vanguard. (2006). *Biometric fingerprint technology will curb identity fraud in Nigeria*. Retrieved from http://www.vanguardngr.com/articles/2002/features/technology/tec525102006.html

Varma, S. (2011). *Preliminary Item Statistics Using Point-Biserial Correlation and P-Values.* Morgan Hill, CA: Educational Data Systems, Inc.

Viadero, D. (2005, January 26). 'Mixed methods' research examined. *Education Week*, *24*(20), 1–20.

Vollmer, B. C. (2006). *Biometrics, RFID technology, and the ePassport: Are Americans risking personal security in the face of terrorism?* (Unpublished master's thesis). Georgetown University, Washington, DC.

Wahid, F. (2007). Using the technology adoption model to analyze internet adoption and use among men and women in Indonesia. *The Electronic Journal on Information Systems in Developing Countries*, *32*(6), 1–8.

Walonick, D. S. (2005). *Elements of a research proposal and report*. Retrieved from http://www.statpac.com/research-papers/research-proposal.htm#chapter-3

Wang, W. T., and Liu, C. H. (n.d.). *The application of the technology acceptance model: A new way to evaluate information system success*. Albany, NY: School of

Information Science and Policy, University at Albany.

Watkins, M. (2007). *Biometrics: Introduction.* Retrieved from http://www.cippic.ca/biometrics/

Wayman, J. L. (2000). *National biometric test center collected works 1997–2000*. San Jose, CA: National Biometric Test Center.

Weber, K. (2006). Privacy invasions: New technology that can identify anyone anywhere challenges how we balance individuals' privacy against public goals. *European Molecular Biology Organization, Vol. 7* (Special Issue), S36–S39.

Westin, A. (2002). *Public attitudes toward the use of biometric identification technologies by government and private sector.* Princeton, NJ: Opinion Research International.

White, R. (2007). Using mixed method and quantitative research methodologies to advise business executives. *Helium.* Retrieved from http://www.helium.com/tm/100943/introductionresearch-scaffolding-industry-capability

Wilcox, N. A., Jr., and Regan, T. M. (2002). Identity fraud: Providing a solution. *Journal of Economic Crime Management, 1*(1), 1–17.

Wong, Y. K., Rubasinghe, A., and Steele, R. (2005). *An empirical research program for biometric technology adoption.* Proceedings of *IRIS: 28 Conference*, Kristiansand, Norway.

Woodard, D. L. (2004). *Exploiting finger surface as a biometric identifier*. (Unpublished

doctoral dissertation). University of Notre Dame, Indiana.

Woods, T. (2009). *The effect of faculty performance measurement systems on student retention.* Retrieved from Business Source Premier database.

Woodward, D., Horn, C., Gatune, J., and Thomas, A. (2003). *Biometrics: A look at facial recognition*. Santa Monica, CA: Rand Publication.

Woodward, J. D. (2001). *Biometrics: Facing up to terrorism*. Santa Monica: CA: Rand Corporation.

Woodward, J. D., Jr. (2005 September-October). Using biometrics to achieve identity dominance in the global war on terrorism, *Military Review* pp. 30–34.

Woodward, J. D., Jr., Christopher H., Gatune, J., & Thomas, A. (2003). *Biometrics: A look at facial recognition*. Santa Monica, CA: Rand Publication.

Woodward, J. D., Jr., Webb, K. W., Newton, E. M., Bradley, M., and Rubenson, D. (2001). *Army biometrics applications: Identifying and addressing sociocultural concerns*. Santa Monica, CA: Rand Publication.

Worldworx Travel. (2009). *Travel safety: Africa: Nigeria*. Retrieved from http://www.worldworx.tv/safety/africa/nigeria/index.htm

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*, *12*(1), 125–137.

Zureik, E., and Hindle, K. (2004). Governance, security, and technology: The case of Biometrics. Studies in Political Economy, 73, 113–137.

Appendix A: Survey Cover Letter

You are invited to participate in this investigation. The study is intended to solicit information on how factors such as ease of use, usefulness, security, and awareness affect the adoption and usability of biometrics technology for reliably recognizing and confirming peoples' identity within developing countries such as Nigeria. The survey will require adults to answer demographic questions and answer short written response answers. To participate in this study you must meet these criteria: (a) you must be 18 years of age or older, and (b) you must not be a user of biometrics technology. The survey will last forty five minutes.

The results of this research will contribute to a clearer understanding of how these factors may contribute to the adoption, implementation, and use of biometrics technique to control identity fraud. The findings may be included in documentation of a doctoral dissertation. They may also be presented in scholarly meetings and published articles. Your identity as a study participant will be strictly confidential and will not be revealed in any materials or presentations. If you are willing to participate, please:

1. Complete Appendixes B and C of this letter.
2. Complete each item on the enclosed survey.
3. Mail the completed survey to:

   2730 Eisenhower Ave

   Alexandria, VA 22314 USA

   Or

   No. 40 Setuga Street, Lagos

You can contact the researcher at the telephone numbers listed below to have the questionnaire picked up. Should you have any questions, you may contact the researcher at 080-358-22582 (Lagos), (703)-867-0104 (USA), or the supervising Professor, Dr. Raghu Korrapati, at rkorrapati@waldenu.edu. Thank you for taking the time to assist me in this study. Your participation is appreciated.

Sincerely,

Gideon U. Nwatu
Researcher and Doctoral Candidate
Walden University

Appendix B: Consent Statement

CONSENT FORM TO PARTICIPATE IN A RESEARCH STUDY

You are invited to take part in a research study about the factors that will affect adoption of biometrics technology such as fingerprint, iris, and face to control identity fraud. You were chosen for the study because you are literate, 18 years of age or older, and familiar about biometrics technology. This form is part of a process called "informed consent" to allow you understand this study before deciding whether to take part.

This study is being conducted by a researcher named Gideon U. Nwatu, who is a doctoral student at Walden University.

Background Information:

The proliferation of information communication technologies (ICTs) has increased the prevalence of identity fraud on a global scale. In 2007, identity fraud generated international attention and negative publicity toward Nigeria and its citizens.

The purpose of this study is to demonstrate that biometrics technology is useful to control identity fraud within Lagos, Nigeria. The technology is reliable to confirm individual characteristics, control crimes for public security, and safety.

Procedures:

If you agree to be in this study, you will be asked to:

- Respond to screening questions
- Answer and submit survey questionnaires that will be given to you

Voluntary Nature of the Study:

Your participation in this study is voluntary. This means that everyone will respect your decision of whether or not you want to be in the study. No one at Walden University will treat you differently if you decide not to be in the study. If you decide to join the study now, you can still change your mind during the study. If you feel stressed during the study you may stop at any time. You may skip any questions that you feel are too personal.

Risks and Benefits of Being in the Study:

The risk involved in this study is minimal, which is the time you will spend to participate in the study. The study is expected to offer the Nigerian government actionable strategies for controlling crime. The dangers and consequences of identity fraud and the threats of terrorism are real and are increasing on a global scale. Biometrics technology, which has been viewed as providing better security, increased efficiency, and more reliable identity assurance than other commonly used methods of authentication/identification based on what a user possesses or what a user knows has potential benefits for identity verification and confirmation.

Compensation:

The participation in this study is voluntary and no compensation is paid to individuals. However, appreciation will be expressed and extended through a "Thank you" note.

Confidentiality:

Any information you provide will be kept confidential. The researcher will not use your information for any purpose outside of this research project. Also, the researcher will not include your name or anything else that could identify you in any reports of the study.

Contacts and Questions:

You may ask any questions you have now. Or if you have questions later, you may contact the researcher via 01 9 703 867-0104, gidudo@att.net, and gnwatu@waldenu.edu If you want to talk privately about your rights as a participant, you can call Dr. Leilani Endicott. She is the Walden University representative who can discuss this with you. Her phone number is 1-800-925-3368, extension 1210. Walden University's approval number for this study is **05-04-10-0209264** and it expires on **May 3, 2011.**

The researcher will give you a copy of this form to keep.

Statement of Consent:

I have read the above information and I feel I understand the study well enough to make a decision about my involvement. By signing below, I am agreeing to the terms described above.

Printed Name of Participant _____

Date of consent _____

Participant's Written or Electronic* Signature _____

Researcher's Written or Electronic* Signature _____

*Electronic signatures are regulated by the Uniform Electronic Transactions Act. Legally, an "electronic signature" can be the person's typed name, their email address, or any other identifying marker. An electronic signature is just as valid as a written signature as long as both parties have agreed to conduct the transaction electronically.

Appendix C: Confidentiality Agreement

I, Gideon U. Nwatu (hereinafter known as the "Researcher"), in the department of Applied Management and Decision Sciences (AMDS) of Walden University is a doctoral candidate conducting a study. The purpose of the investigation is to explore whether ease of use, security, perceived usefulness, and users' perceptions will potentially contribute to the adoption and implementation of biometrics techniques to control identity fraud (IDf) in developing countries such as Nigeria. Data from this research may be used to formulate policies to encourage the use of biometrics technology such as fingerprint and iris scans in the private and public sectors to safeguard individual security and control crimes.

To conduct the study, I agree to:

1. Keep all the information shared with me confidential and not to discuss or disclose such information in any form with anybody.
2. Maintain and secure the data in my custody.
3. Only use the data obtained from you for the purposes of conducting the investigation.

This agreement regarding confidentiality and use obligations shall remain in effect during and after termination of this agreement for a period of five years from the date you accept, as indicated below.

This agreement constitutes the understanding of you, the participant, and I, the researcher with respect to the information hereto. If you have any questions, you may contact me at gnwatu@waldenu.edu or the supervising Chairperson, Dr. Raghu Korrapati at rkorrapati@waldenu.edu.

Please show your acceptance and agreement to the aforementioned terms and sign this letter of agreement in the space below.

Sincerely,

Gideon U. Nwatu
Doctoral/research student

Agreed and Accepted
By:_____

Title:_____

Date_____

Appendix D: Demographical and Awareness Questionnaire

The purpose of this survey is to collect information on barriers affecting the adoption and usability of biometrics technology, such as fingerprint, to control identity fraud.

The survey is divided into five sections. The first asks for demographical information and evaluates your knowledge of biometrics. The second, third, and fourth sections rate your responses about ease of use, perceived usefulness, and security, respectively. The fifth section in this investigation asks for your comments, observations, or insights that may be useful concerning biometrics technology.

In sections 1 through 4, please answer the questions and place an "X" in the designated location that provides the most accurate answer. All responses are confidential and will be used only in conjunction to this research.

Section 1

1.	Gender:	☐	Female	☐	Male		
2.	Current Age	☐	24–40 Years	☐	41–60 Years	☐	Over 61 Years
3.	Educational Level:	☐	High School	☐	College Grad	☐	Master s/PhD
4.	Do you have knowledge of biometrics technology?					☐	Yes ☐ No
5.	Do you know that biometrics can be used to identify people?					☐	Yes ☐ No
6.	Do you have the knowledge of fingerprint technology?					☐	Yes ☐ No
7.	Do you have the knowledge of iris scan?					☐	Yes ☐ No
8	Do you accept the use of fingerprint technology for identification?					☐	Yes ☐ No

9. Do you accept the use of iris scan technique for verification? ☐ Yes ☐ No

10. Do you accept the adoption of biometrics technology to control identity fraud? ☐ Yes ☐ No

Section 2

This section relates to your response to the ease of use of biometrics technology. With each statement, please indicate your response and place an "X" in the column that best matches the degree to which you agree or disagree with the statement.

Survey Statement	SA	A	NC	D	SD
1. I can personally use biometrics technology.					
2. I would feel comfortable using biometrics technology.					
3. I could follow instructions easily to use biometrics technology.					
4. I would be able to use biometrics technology to protect my identity.					
5. Using biometrics technology is far too complicated for me.					
6. I would like to use biometrics technology if it is not difficult.					
7. I would not use biometrics technology if it is complex.					
8. I would like instructions to be provided on how to use biometrics technology.					
9. Information about the system would help me make a decision to use it.					

Note: SA = Strongly Agree; A = Agree; NC = No Comment; D = Disagree; SD = Strongly Disagree

Section 3

This section relates to your response regarding the usefulness of biometrics technologies such as fingerprint technique or iris scan to control identity fraud. With each statement, please indicate your response and place an "X" in the column that best matches the degree to which you agree or disagree with the statement.

Survey Statement	SA	A	NC	D	SD
1. Using biometrics technology to verify identity is a good idea.					
2. Using biometrics technology to prevent identity fraud is a clever idea.					
3. I like the idea of using biometrics technology for identification.					
4. I would like to use biometrics technology to protect my banking transactions.					
5. Using biometrics technology to identify criminals is a good idea.					

Note: SA = Strongly Agree; A = Agree; NC = No Comment; D = Disagree; SD = Strongly Disagree.

Section 4

This section relates to your level of awareness regarding the adoption and use of biometrics technologies such as fingerprint and iris scan. With each statement, please indicate your response by placing an "X" in the column that best matches the degree to which you agree or disagree with the statement.

Survey Statement	SA	A	NC	D	SD
1. I have seen, heard, or read about biometrics technology such as fingerprint and iris scan.					
2. I have been exposed to biometrics technology such as fingerprint and iris scan.					
3. I am aware of the benefits of biometrics technology such as fingerprint and iris scan.					
4. I know how biometrics technology can be used in daily life.					

Note: SA = Strongly Agree; A = Agree; NC = No Comment; D = Disagree; SD = Strongly Disagree.

Section 5

This section relates to your concerns about security in relationship to the adoption and use of biometrics security systems such as fingerprint and iris scan. With each statement, please indicate your response and place an "X" in the column that best matches the degree to which you agree or disagree with the statement.

Survey Statement	SA	A	NC	D	SD
1. I am not interested in using fingerprint technique for identification.					
2. I am not interested in using the iris scan for identification.					
3. I have no need for fingerprint technology.					
4. I have no need for the iris scan.					
5. I would use biometrics technology to protect my identity.					
6. I can protect my identity without the iris scan security system.					
7. I would use fingerprint technology for banking services.					
8. I would use iris scan technology for banking services.					
9. I have been a victim of identity fraud.					
10. I would like biometrics technology to be used to control identity fraud.					

Note: SA = Strongly Agree; A = Agree; NC = No Comment; D = Disagree; SD = Strongly Disagree

Appendix E: Interview Protocol

CONSENT FORM FOR AN INTERVIEW IN A RESEARCH STUDY

You are invited to take part in a research study about the factors that will affect adoption of biometrics technology such as fingerprint, iris, and face to control identity fraud. You were chosen for the study because you are literate, 18 years of age or older, and familiar about biometrics technology. This form is part of a process called "informed consent" to allow you understand this study before deciding whether to take part.

This study is being conducted by a researcher named Gideon U. Nwatu, who is a doctoral student at Walden University.

Background Information:

The proliferation of information communication technologies (ICTs) has increased the prevalence of identity fraud on a global scale. In 2007, identity fraud generated international attention and negative publicity toward Nigeria and its citizens.

The purpose of this study is to demonstrate that biometrics technology is useful to control identity fraud within Lagos, Nigeria. The technology is reliable to confirm individual characteristics, control crimes for public security, and safety.

Procedures:

If you agree to be in this study, you will be asked to:

- Respond to screening questions
- Participate in a semi-structured interview
- Duration of interview is between 30–45 minutes

Voluntary Nature of the Study:

Your participation in this study is voluntary. This means that everyone will respect your decision of whether or not you want to be in the study. No one at Walden University will treat you differently if you decide not to be in the study. If you decide to join the study now, you can still change your mind during the study. If you feel stressed during the study you may stop at any time. You may skip any questions that you feel are too personal.

Risks and Benefits of Being in the Study:

The risk involved in this study is minimal, which is the time you will spend to participate in the study. The study is expected to offer the Nigerian government actionable strategies for controlling crime. The dangers and consequences of identity fraud and the threats of terrorism are real and are increasing on a global scale. Biometrics technology, which has been viewed as providing better security, increased efficiency, and more reliable identity assurance than other commonly used methods of authentication/identification based on what a user possesses or what a user knows has potential benefits for identity verification and confirmation.

Compensation:

The participation in this study is voluntary and no compensation is paid to individuals. However, appreciation will be expressed and extended through a "Thank you" note.

Confidentiality:

Any information you provide will be kept confidential. The researcher will not use your information for any purpose outside of this research project. Also, the researcher will not include your name or anything else that could identify you in any reports of the study.

Contacts and Questions:

You may ask any questions you have now. Or if you have questions later, you may contact the researcher via 01 9 703 867-0104, gidudo@att.net, and gnwatu@waldenu.edu If you want to talk privately about your rights as a participant, you can call Dr. Leilani Endicott. She is the Walden University representative who can discuss this with you. Her phone number is 1-800-925-3368, extension 1210. Walden University's approval number for this study is **05-04-10-0209264** and it expires on **May 3, 2011.**

The researcher will give you a copy of this form to keep.

Statement of Consent:

I have read the above information and I feel I understand the study well enough to make a decision about my involvement. By signing below, I am agreeing to the terms described above.

Printed Name of Participant _____

Date of consent _____

Participant's Written or Electronic* Signature _____

Researcher's Written or Electronic* Signature _____

*Electronic signatures are regulated by the Uniform Electronic Transactions Act. Legally, an "electronic signature" can be the person's typed name, their email address, or any other identifying marker. An electronic signature is just as valid as a written signature as long as both parties have agreed to conduct the transaction electronically.

Interview Protocol

Research Questions	Interview Questions

1. What is the relationship between ease of use and user perceptions toward adoption of biometrics technology for control of identity fraud?	How difficult do you think the use of fingerprint is? Potential follow up question: Are you willing to adopt biometrics technology if it easy to use? On users' perceptions toward adoption of biometrics. Do you think that adults will use biometrics technology if it is easy to use? Potential follow up question: Do you think that individuals will use the technology if they believe it is easy to learn? Would you use biometrics if it is useful?
2. To what extent, if any, is biometrics technique considered an effective mechanism for identity verification; and what is the relationship between perceived usefulness and acceptance of biometrics technology for control of identity deception?	Potential follow up question: Do you think that users will accept fingerprint and iris scans for their usefulness to achieve verification and control identity management? Do you think biometrics technology can protect your personal identity?
3. What is the relationship between security and user perception toward adoption of biometrics system for control of identity fraud?	Potential follow up questions: Do you think that the adoption of fingerprint technology will minimize the rate at which documents are forged? Do you think that biometrics is beneficial in banking transactions?
4. What is the relationship between awareness and the adoption of biometrics technology for control of identity deception?	Are you aware of biometrics technology such as fingerprint and iris scan? Potential follow up questions: Are you familiar about how biometrics technology is used to identify people? How did you know about biometrics?

Thank participant for participating in the interview. Assure participant of the confidentiality of information provided and the potential for a follow-up interview

Appendix F: IRB Notice of Approval to Conduct Research

Subject: Notification of Approval to Conduct Research-Gideon Nwatu
From: <IRB@waldenu.edu>
Date: Tue, 4 May 2010 12:46:18 -0500
To: <gnwatu@waldenu.edu>
CC: <research@waldenu.edu>, <Raghu.Korrapati@waldenu.edu>

Dear Mr. Nwatu,

This email is to serve as your notification that Walden University has approved BOTH your dissertation proposal and your application to the Institutional Review Board. As such, you are approved by Walden University to conduct research.

Please contact the Office of Student Research Support at research@waldenu.edu if you have any questions.

Congratulations!

Jenny Sherer
Operations Manager, Office of Research Integrity and Compliance

Leilani Endicott
IRB Chair, Walden University

Appendix G: IRB Materials Approved

Subject: IRB materials approved-Gideon Nwatu
From: <IRB@waldenu.edu>
Date: Tue, 4 May 2010 12:45:44 -0500
To: <gnwatu@waldenu.edu>
CC:<research@waldenu.edu>, <Raghu.Korrapati@waldenu.edu>

Dear Mr. Nwatu,

This email is to notify you that the Institutional Review Board (IRB) has approved your application for the study entitled, "Biometrics Technology: Understanding Dynamics Influencing Adoption for Control of Identification Deception Within Nigeria."

Your approval # is 05-04-10-0209264. You will need to reference this number in your dissertation and in any future funding or publication submissions. Also attached to this e-mail are the IRB approved consent forms. Please note, if these are already in an on-line format, you will need to update the consent documents to include the IRB approval number and expiration date.

Your IRB approval expires on May 3, 2011. One month before this expiration date, you will be sent a Continuing Review Form, which must be submitted if you wish to collect data beyond the approval expiration date.

Your IRB approval is contingent upon your adherence to the exact procedures described in the final version of the IRB application document that has been submitted as of this date. If you need to make any changes to your research staff or procedures, you must obtain IRB approval by submitting the IRB Request for Change in Procedures Form. You will receive an IRB approval status update within 1 week of submitting the change request form and are not permitted to implement changes prior to receiving approval. Please note that Walden University does not accept responsibility or liability for research activities conducted without the IRB's approval, and the University will not accept or grant credit for student work that fails to comply with the policies and procedures related to ethical standards in research.

When you submitted your IRB application, you a made commitment to communicate both discrete adverse events and general problems to the IRB within 1 week of their occurrence/realization. Failure to do so may result in invalidation of data, loss of academic credit, and/or loss of legal protections otherwise available to the researcher.

Both the Adverse Event Reporting form and Request for Change in Procedures form can

be obtained at the IRB section of the Walden web site or by emailing irb@waldenu.edu: http://inside.waldenu.edu/c/Student_Faculty/StudentFaculty_4274.htm

Researchers are expected to keep detailed records of their research activities (i.e., participant log sheets, completed consent forms, etc.) for the same period of time they retain the original data. If, in the future, you require copies of the originally submitted IRB materials, you may request them from Institutional Review Board.

Please note that this letter indicates that the IRB has approved your research. You may not begin the research phase of your dissertation, however, until you have received the **Notification of Approval to Conduct Research** (which indicates that your committee and Program Chair have also approved your research proposal). Once you have received this notification by email, you may begin your data collection.

Both students and faculty are invited to provide feedback on this IRB experience at the link below:

http://www.surveymonkey.com/s.aspx?sm=qHBJzkJMUx43pZegKlmdiQ_3d_3d

Sincerely,
Jenny Sherer, M.Ed.
Operations Manger
Office of Research Integrity and Compliance
Email: irb@waldenu.edu
Fax: 626-605-0472
Tollfree : 800-925-3368 ext. 1341
Office address for Walden University:
155 5th Avenue South, Suite 100
Minneapolis, MN 55401

Appendix H: Sample of Interview Comments

If biometrics technology is not complex to use, [the] majority of people will be interested to use [*sic*] it in banking transactions to protect financial records.

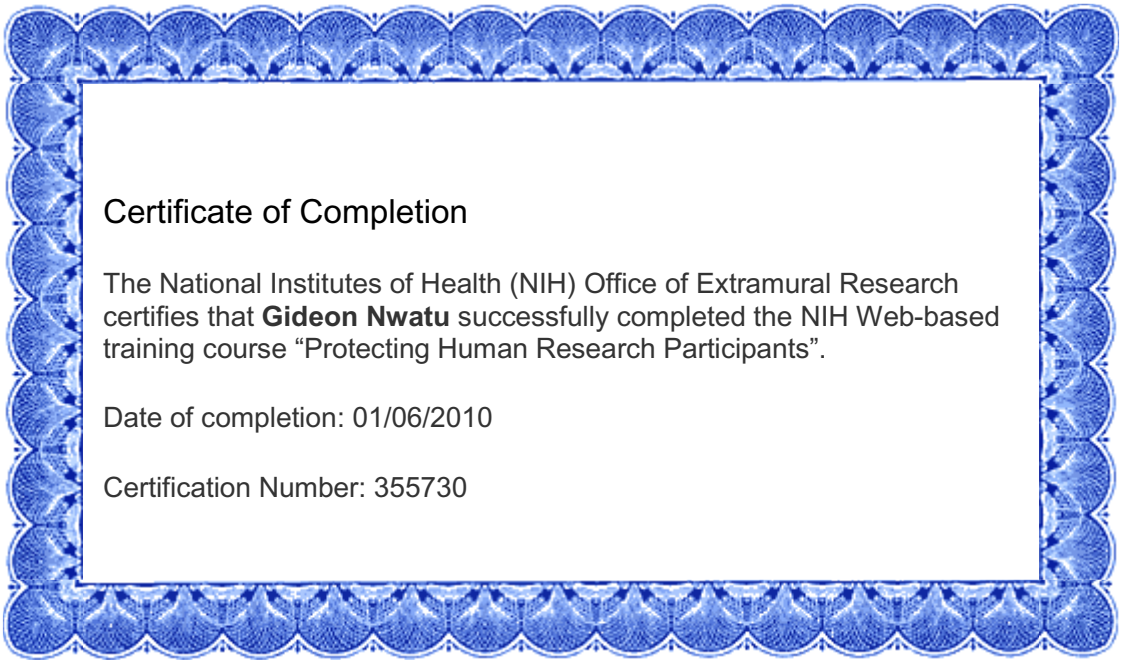
Maybe this technology was needed to identify registered voters to avoid voter fraud. Biometrics technology will be helpful to manage [*sic*] identity and hold individuals responsible when they commit crimes.

The implementation of [a] biometrics technique seemed to be a good idea but there must be awareness for [*sic*] the benefits so that people become familiar about [*sic*] it and develop favorable attitude[s] that will encourage its adoption.

Practically speaking, I would tend to use the technology for the protection of my identity but worry if the biometrics data was stolen.

I am concerned [about] what happens if the wrong person is not correctly identified and, as a result, the individual is allowed to have access to restricted data.

Appendix I: The National Institute of Health (NIH) Certificate of Completion



Certificate of Completion

The National Institutes of Health (NIH) Office of Extramural Research certifies that **Gideon Nwatu** successfully completed the NIH Web-based training course "Protecting Human Research Participants".

Date of completion: 01/06/2010

Certification Number: 355730

Appendix J: Items for Research Question 1: Ease of Use

Item 1

I can personally use biometrics technology

		Frequency	Percent	Valid percent	Cumulative percent
Valid	Disagree	69	57	57	57
	No comment	13	11	11	68
	Agree	38	32	32	100
	Total	120	100	100	

Item 2

I would feel comfortable using biometrics technology

		Frequency	Percent	Valid percent	Cumulative percent
Valid	Disagree	53	44	44	57
	No comment	6	5	5	68
	Agree	61	51	51	100
	Total	120	100	100	

Item 3

I could follow instructions easily to use biometrics technology

		Frequency	Percent	Valid percent	Cumulative percent
Valid	Disagree	3	3	3	3
	No comment	6	5	5	8
	Agree	111	92	92	100
	Total	120	100	100	

Item 4

I would be able to use biometric technology to protect my identity

		Frequency	Percent	Valid percent	Cumulative percent
Valid	Disagree	30	25	25	25
	No	27	22	22	47

I would be able to use biometric technology to protect my identity					
	comment				
	Agree	63	53	53	100
	Total	120	100	100	

Item 5

Using biometric technology is far too complicated for me					
		Frequency	Percent	Valid percent	Cumulative percent
Valid	Disagree	26	22	22	22
	No comment	10	8	8	20
	Agree	84	70	70	100
	Total	120	100	100	

Item 6

I would like to use biometrics technology if it is not too difficult					
		Frequency	Percent	Valid percent	Cumulative percent
Valid	Disagree	69	57	57	57
	No comment	13	11	11	68
	Agree	38	32	32	100
	Total	120	100	100	

Item 7

I would not use biometrics technology if it is complex					
		Frequency	Percent	Valid percent	Cumulative percent
Valid	Disagree	16	13	13	13
	No comment	9	8	8	21
	Agree	95	79	79	100
	Total	120	100	100	

Item 8

I would like instructions to be provided on how to use biometrics technology

		Frequency	Percent	Valid percent	Cumulative percent
Valid	Disagree	2	2	2	2
	No comment	5	4	4	6
	Agree	113	94	94	100
	Total	120	100	100	

Item 9

Information about the system would help me make a decision to use it

		Frequency	Percent	Valid percent	Cumulative percent
Valid	Disagree	0	0	0	0
	No comment	1	1	1	1
	Agree	119	99	99	100
	Total	120	100	100	

Appendix K: Items for Research Question 2: Perceived Usefulness

Item 1

Using biometrics technology to verify identity is a good idea

		Frequency	Percent	Valid percent	Cumulative percent
Valid	Disagree	8	7	7	7
	No comment	5	4	4	11
	Agree	107	89	89	100
	Total	120	100	100	

Item 2

Using biometrics technology to prevent identity fraud is a clever idea

		Frequency	Percent	Valid percent	Cumulative percent
Valid	Disagree	33	28	28	28
	No comment	49	40	40	68
	Agree	38	32	32	100
	Total	120	100	100	

Item 3

I like the idea of using biometrics technology for identification

		Frequency	Percent	Valid percent	Cumulative percent
Valid	Disagree	3	3	3	3
	No comment	5	4	4	7
	Agree	112	93	93	100
	Total	120	100	100	

Item 4

I would like to use biometrics technology to protect my banking transactions

	Frequency	Percent	Valid percent	Cumulative

I would like to use biometrics technology to protect my banking transactions					
					percent
Valid	Disagree	40	33	33	33
	No comment	34	28	28	61
	Agree	46	39	39	100
	Total	120	100	100	

Item 5

Using biometrics technology to identify criminals is a good idea					
		Frequency	Percent	Valid percent	Cumulative percent
Valid	Disagree	0	0	0	0
	No comment	2	2	2	2
	Agree	118	98	98	100
	Total	120	100	100	

Appendix L: Items for Research Question 3: Security Concern

Item 1

I am not interested in using fingerprint techniques for identification					
		Frequency	Percent	Valid percent	Cumulative percent
Valid	Disagree	120	100	100	100
	No comment	0	0	0	0
	Agree	0	0	0	100
	Total	120	100	100	

Item 2

I am not interested in using the iris scan for identification					
		Frequency	Percent	Valid percent	Cumulative percent
Valid	Disagree	68	56	56	56
	No comment	26	22	22	78
	Agree	26	22	22	100
	Total	120	100	100	

Item 3

I have no need for fingerprint technology					
		Frequency	Percent	Valid percent	Cumulative percent
Valid	Disagree	84	70	70	70
	No comment	27	22	22	92
	Agree	9	8	8	100
	Total	120	100	100	

Item 4

I have no need for iris scan					
		Frequency	Percent	Valid percent	Cumulative percent
Valid	Disagree	58	48	48	48
	No	43	36	36	84

I have no need for iris scan					
	comment				
	Agree	19	16	16	100
	Total	120	100	100	

Item 5

I would use biometrics technology to protect my identity					
		Frequency	Percent	Valid percent	Cumulative percent
Valid	Disagree	10	8	8	8
	No comment	5	4	12	44
	Agree	105	88	88	100
	Total	120	100	100	

Item 6

I can protect my identity without the iris scan security system					
		Frequency	Percent	Valid percent	Cumulative percent
Valid	Disagree	13	11	11	11
	No comment	58	48	48	59
	Agree	49	41	41	100
	Total	120	100	100	

Item 7

I would use fingerprint technology for banking services					
		Frequency	Percent	Valid percent	Cumulative percent
Valid	Disagree	7	6	6	6
	No comment	14	12	12	18
	Agree	99	82	82	100
	Total	120	100	100	

Item 8

I would use iris scan technology for banking services					
		Frequency	Percent	Valid percent	Cumulative percent
Valid	Disagree	50	42	42	42
	No comment	47	39	39	81
	Agree	23	19	19	100
	Total	120	100	100	

Item 9

I have been a victim of identity fraud					
		Frequency	Percent	Valid percent	Cumulative percent
Valid	Disagree	9	8	8	8
	No comment	54	45	45	53
	Agree	57	47	47	100
	Total	120	100	100	

Item 10

I would like biometrics technology to be used to control identity fraud.					
		Frequency	Percent	Valid percent	Cumulative percent
Valid	Disagree	1	1	1	1
	No comment	1	1	1	2
	Agree	118	98	98	100
	Total	120	100	100	

Appendix M: Items for Research Question 4: Awareness

Item 1

I have seen, heard or read about biometrics technology such as fingerprint and iris scan

		Frequency	Percent	Valid percent	Cumulative percent
Valid	Disagree	4	3	3	3
	No comment	0	0	0	3
	Agree	116	97	97	100
	Total	120	100	100	

Item 2

I have been exposed to biometrics technology, such as fingerprint and iris scan

		Frequency	Percent	Valid percent	Cumulative percent
Valid	Disagree	20	17	17	17
	No comment	37	31	31	48
	Agree	63	52	52	100
	Total	120	100	100	

Item 3

I know how biometrics technology can be used in daily life

		Frequency	Percent	Valid percent	Cumulative percent
Valid	Disagree	30	25	25	25
	No comment	29	24	24	49
	Agree	61	51	51	100
	Total	120	100	100	

Item 4

I know how biometrics technology can be used in daily life

	Frequency	Percent	Valid percent	Cumulative percent

I know how biometrics technology can be used in daily life					
Valid	Disagree	29	24	24	24
	No comment	13	11	11	35
	Agree	78	65	65	100
	Total	120	100	100	

Curriculum Vitae

GIDEON U. NWATU, MBA, SECURITY+, ITIL V3, MCSE, MCT, MCP+I, MCP.

☎ 703-867-0104 💻 gideon.nwatu@gmail.com

INFORMATION TECHNOLOGY ~ QUALITY ASSURANCE ~ IT INSTRUCTOR

Motivated, forward-thinking, and performance-driven professional with breadth of backgrounds and competencies for providing high-quality technology solutions and services to the satisfaction of end users/clients while contributing significant impact to corporate and organizational values. Demonstrated strengths to perform independently and the ability to nurture partnerships within and across team boundaries ensuring success in delivering results. Offered capabilities for state-of-the art technology implementation in installations, configurations, documentations, testing, training, troubleshooting, and quality assurance. Blended more than twelve years of business principles, information technology, and enhancing professional potentials to contribute and truly be an integrated asset for achievability of mission critical objectives and customers' satisfaction.

Performance Milestones

- ✓ Applied information assurance vulnerability alerts (IAVAs) patches on hosts
- ✓ Prepared high level program monthly reports (PMRs) presented and submitted to the customer
- ✓ Executed Security Readiness Review (SRR); pre-scanned hosts, which exposed network vulnerability that prompted mitigation
- ✓ Maintained information systems security as increasingly critical to mission, operation, and protection of network infrastructures
- ✓ Implemented security policies on platforms, which enforced access control
- ✓ Provided quarterly instructional
- ✓ Managed Remote Query Application that provided a web-based search capability for identification of suspected criminals
- ✓ Researched best practices in the Service Desk industry and made recommendation
- ✓ Evaluated software/application that linked the names of individuals with criminal records
- ✓ Identified and implemented control measures that decreased software errors, which assured quality, increased combat communication, and effectiveness
- ✓ Wrote Functional Test Plan at, which was used to validate messaging systems objectives
- ✓ Developed Test Plan Templates,

services and saved more than 10 % of hiring and administrative costs	which significantly reduced time cycle of generating reports

ACADEMIC CREDENTIALS

PhD Candidate, All But Dissertation (ABD), Information Systems Management (ISM)/Biometrics Technology, Walden Univ., Minneapolis, MN **(Spring 2011)**
MBA, Management & Accounting, Univ. of District of Columbia, Washington, DC **(1991)**
BS, Business Administration, West Virginia Univ., Morgantown, WV **(1983)**

Employment Profile

Advanced Systems Development (ASD), Inc., Arlington, VA, October 2009-Present.
Strayer University, Alexandria, VA, January 2000-Present.
Raytheon Intelligence and Information Systems, Falls Church, VA, January 2008-Oct. 2009.
The Analysis Corporation, McLean, VA, May-December 2007.
Computer Sciences Corporation, Chantilly, VA, Jan. 2004-January 2007.
DynCorp, Chantilly, VA, March 2002-December 2003.
Titan Systems Corporation, Validity Division, Largo, MD, March 1999-March 2002.

AWARD / RECOGNITION / AFFILIATION

Raytheon Intelligence & Information Systems
Golden Eagle ~ Joint Interoperability Test Command (JITC)
Strayer University
International Association for Counterterrorism & Security Professionals

Scope of Professional Progression

INFORMATION TECHNOLOGY QUALITY ASSURANCE (IT QA), *Advanced Systems Development (ASD), Inc., Arlington, VA, October 2009-Present.*

- Extract data from BMC Remedy to trend performance in the following areas: program management, engineering support, enterprise systems availability, monthly failover, system backups, on call support, daily status, incident management and service requests, customer call backs, IAVA, and STIG compliance
- Provide technical and process guidance for quality service for users' satisfaction
- Coordinate with Technical Managers and Team Leads to track issues for prompt resolution
- Evaluate the activities of the Service Desk Personnel
- Investigate, calculate, and report matrices
- Develop program management report (PMR)
- Research best practices in the Service Desk Industry
- Review call services and make recommendations to improve customers' contentment
- Provide input to service request remediation

- Present data and evaluate if terms of Service Level Agreements (SLAs) are met
- Contact users and validate service request status (SRS)
- Assess organizational training plan (OTP) to improve quality of the artifact
- Verify quantitative measurements in support of IT services contract
- Analyze backlog of customer requests and incidents to ascertain effective strategy for resolution

SENIOR QUALITY ASSURANCE ENGINEER I, *Raytheon Intelligence & Information Systems (IIS), Falls Church, VA, Jan. 2008- October, 2009*

- Responsible for assigned programs, which ensured projects are executed within budgetary and contract requirements
- Prepared and interpreted mission assurance risk calculator (MARC) that depicted monthly program status: green/yellow/red
- Evaluated adequacy of software readiness for baseline development, which minimized defects
- Participated in meetings with Program Manager (PM), Program Engineer (PE), Software Engineer (SE), Hardware Engineer (HE), Testers, and resolved change requests (CRs) and documented defects
- Managed, monitored program, and assessed status of projects that reflected tasks assignments, schedules, and financial resources
- Verified that software baselines are created on Digital Video Disks (DVDs), which were sent to the customer along with Contract Data Requirement List (CDRL)
- Compiled and analyzed relevant material evidence that prompted remedies of audit deficiencies
- Contributed in Risk Review Board (RRB) meetings, discussed, and assessed risks captured, which provided lessons learned
- Conducted and documented internal audit findings for conformity and non-conformity of the quality system elements with specified requirements
- Examined program configuration changes, prioritized risks, and opportunities
- Issued reports of audit short coming, which warranted timely actions
- Ascertained the effectiveness of the quality system and identified opportunities for mitigation
- Contributed measures to Configuration Control Board (CCB) meetings and demonstrated commitment to process improvement
- Pinpointed weaknesses that might impact process effectiveness and provided improvement strategies to assure quality standards to minimize customer complaints
- Reviewed relevant standards for integrity of artifacts and work products to ensure compliance of documented processes
- Validated conformance of Quality Management System practices to customer mandated value requirements
- Provided documentation evaluations/examinations for clarity, compliance with standards, which ensured readability, and overall quality products delivered to the customer

ADJUNCT INSTRUCTOR, *Strayer University, Alexandria, VA, Jan. 2000-Present.*

- Taught TCP/IP, NT4 technologies, Windows 2000 Server, Professional, and Network Essentials
- Provided quarterly training services to students and saved more than 10% of hiring and administrative costs
- Currently teaching Windows 2003 Server, XP Professional, Network Infrastructure, Business Data Communications, Active Directory Services, Introduction to Networking, Network Security, Service-Oriented Architecture (SOA), and Computer Forensics
- Update course syllabi; install, configure, and troubleshoot operating systems used for lectures and laboratory exercises
- Assign/delegate "hands-on" sessions; administer quizzes, examinations, projects, and award final grades to students
- Counsel and mentor students, which support course and program completion

QUALITY ASSURANCE/SYSTEMS TEST ENGINEER*, The Analysis Corporation, McLean, VA, May-Dec. 2007.*

- Developed Test Plan Templates, which significantly reduced time cycle of generating reports
- Managed Remote Query Application that provided a web-based search capability for identification of suspected personalities
- Evaluated software/application that linked the names of individuals with criminal records
- Tested, managed, software/applications that screened, and verified the identity of suspected criminals
- Conferenced and strategized with Developers, Database Administrators, Business Analysts, Software Engineers, Programmers, and Testers the optimal resolution of software/application bugs/defects
- Executed manual, automated tests in Mercury Quality Center, and evaluated software requirements and functionalities
- Analyzed and determined operational and practical capabilities of technologies that assisted in the war on terror
- Extracted on Excel spreadsheet and analyzed software defects used for development and improvement
- Created System Test Plan Templates that conformed to Institute of Electrical and Electronics Engineers (IEEE) standard
- Met with customer's representatives and discussed application requirements
- Reviewed requirements for testability, which minimized errors
- Communicated with development and business teams and evaluated and resolved defects based on priorities
- Wrote, maintained, and executed test cases based on requisites and use
- Calculated and quantified test effort hours, which were used to monitor budget performance of project

SYSTEMS ADMINISTRATOR / TESTER, *Computer Sciences Corporation, Chantilly, VA*, *Jan. 2004-Jan. 2007*

- Set up and configured Domain Controllers, Windows 2000/XP Professional, and Outlook clients used for messaging

- Diagnosed and resolved IP network-related bottlenecks for quality transmission
- Managed network systems that included installation, operation, anti-virus, maintenance, and recoverability through system backups
- Executed Security Readiness Review (SRR), pre-scanned hosts, which exposed network vulnerability that prompted mitigation
- Applied information assurance vulnerability alerts (IAVAs) patches, which assured compliance of DISA standards
- Maintained information systems security as increasingly critical to mission, operation, and protection of network infrastructures
- Created, managed, and deleted user accounts, and updated system security policies on platforms, which enforced access control policies
- Edited vendors' operating systems installation and administration manuals, which eliminated ambiguities
- Coordinated with external locations, established transition states, created, maintained transition schedules, and documented results
- Understood and safeguarded customer's information and network assets that assured sensitive data handling compliance
- Mounted application software programs on LAN and provided guidance to peers about LAN administration procedures

SENIOR SYSTEMS ANALYST, *DynCorp, Chantilly, VA, Mar. 2002-Dec. 2003*

- Validated transition and deployment of Defense Message System (DMS) Release from 2.2 to 3.0; confirmed functionality, and interoperability
- Identified and implemented control measures that decreased software errors, which assured quality, increased combat communication, and effectiveness
- Wrote Functional Test Plan at Joint Interoperability Test Command, which was used to validate messaging systems objectives
- Provided solutions to customer's problems for verification and operational evaluation
- Conducted tests and provided input on projects and programs related to strategic and tactical Command, Control, Communication, Computer, and Intelligence (C4I) Systems
- Utilized assessment methodologies, conducted DMS Functional, Operational, and Acceptance testing
- Wrote Test Incident Reports (TIRs) that compelled software vendors to rectify application bugs

SYSTEMS ANALYST, *Titan Systems Corporation, Validity Division, Largo, MD, Mar. 1999-Mar. 2002*

- Prepared technical analyses, evaluated test data, and procedures for systems after component testing
- Determined performance was in compliance with stated criteria and specifications
- Installed/configured NT4 Member Servers, Domain Controllers, Exchange 5.5 Servers, and desk top clients used for organizational messaging
- Managed communication components, identified bottlenecks, implemented diagnostic actions, and resolutions

- Validated systems interoperability, executed DMS script, and assessed systems and network hosts for vulnerabilities
- Executed functionality tests, which verified Recommended Standard Operating Procedures (RSOPs)

TECHNICAL CERTIFICATIONS

Information Technology Infrastructure Library v3
Microsoft Certified Professional
Microsoft Certified Trainer
Microsoft Certified Professional & Internet
Microsoft Certified Systems Engineer
Microsoft Certified Professional
CompTIA Security+

PROFESSIONAL DEVELOPMENT

Anti-Terrorism Level 1 Awareness, **2011**
CompTIA Security+, **2010**
Annual Counterintelligence, **2010**
DoD Information Assurance Awareness, Annual Certification **2010**
National Capital Region (NCR) Operations Security (OPSEC) **2010**
Team Building/Customer Networking **2010**
Information Assurance Awareness, Annual Certification **2010**
Achieving Customer Service Excellence **2009**
Information Technology Infrastructure Library (ITIL) **2009**
National Capital Region (NCR) Operations Security (OPSEC) **2009**
Privacy Act and DoD Information Assurance Awareness **2009**
Truth in Negotiation Act (TINA), **2009**
Earned Value Management System (EVMS) Level 1, **2009**
Governments Contracts: An Overview, **2009**
Annual DoD Security Training, **2009**
Introduction to Earned Value Management (EVM), **2009**
Common Process Architecture (CPA), **2008**
Fundamentals of Leadership, **2008**
AS 9100 for Internal Audits, **2008**
Basic Labor Charging, **2008**
Business Ethics for Software Compliance, **2008**
DoD Earned Value Management Systems (EVMS) Tripwire Metrics, **2008**
Export Control Awareness, **2008**
Enterprise Security Services: Information Security Awareness, **2008**
Harrington Quality Management System (HQMS), **2008**
Information Security Awareness: Annual Certification, **2008**
Classification Management, National Security Information (NSI), Department of National Intelligence (DNI), **2007**
Sensitive Compartmented Information (SCI), Department of National Intelligence (DNI), **2007**

Operations Security, FBI, In-house, **2007**
Spear - Phishing Awareness, JITC, In-house, **2007**
Anti-Terrorism and Information Assurance Awareness, Department of Defense, In-house, **2005, 2006**
Microsoft Exchange Cluster Server: Installation and Configuration Procedures, Lockheed Martin, Manassas, VA, **2005**
Certified Information Systems Security Professional (CISSP), Intense School, Ft. Lauderdale, FL, **2002**
Windows 2000 MCSE Upgrade Boot Camp: Wave Technologies, Reston, VA, **2001**
E-commerce: Introduction, Framework, and Operational Information Systems Security, **2000**
Introduction to Cisco Router Configuration, Automation Research, Alexandria, VA, **1999**
Train-The-Trainer, Bradley & Associates Inc., Vienna, VA, **1999**
Introduction to UNIX: Information Technology Advanced Training, Vienna, VA, **1999**
Technical Writing: Joint Interoperability Test Command, Indian Head, MD, **1999**

TECHNICAL SKILLS

Information Technology Infrastructure Library (ITIL) v3, Windows 2000/2003 Servers, 2000/XP Professional, Network Infrastructure, Active Directory Services, Microsoft Exchange Server 5.5, 2000, 2003, X. 400, X.500, Windows NT4 Servers, Workstations, Lotus Notes 7.0, UNIX, Oracle 10g, Directory Browser, Global Address List, DNS, TCP/IP, DHCP, FORTEZZA Cards, HP Proliant, Dell PowerEdge, Optiplex, DUNN, and Gateway.

TOOLS/APPLICATIONS

Snagit, Microsoft Word, Outlook, Excel, Power Point, Avaya Call Management System (CMS) Supervisor, V. 14.0.1A.04, BMC Remedy, Mercury Quality Center/Quick Test Professional, Formal Inspection Online Tool, (FIOT), Enterprise Quality Management System (EQMS), IBM Sametime, and mission assurance risk calculator (MARC).