EXPANDING BIOMETRIC COLLECTION IN LAW ENFORCEMENT TO INCLUDE IRIS COLLECTION

Approved: Dr. Cheryl Banachowski-Fuller Date: December 6, 2009
Advisor

EXPANDING BIOMETRIC OPERATIONS IN LAW ENFORCEMENT TO INCLUDE IRIS COLLECTION

A Seminar Paper

Presented to the Graduate Faculty

University of Wisconsin – Platteville

In Partial Fulfillment of the

Requirements for the Degree

Master of Science in Criminal Justice

Jeremiah T. Bruce

December 2009

Acknowledgements

The completion of this paper and degree has been a long endeavor that has finally come to an end, and during this journey there are several people I must acknowledge.

To my beautiful wife, Erin, and our wonderful children Alexis and Aiden: Your constant support has been a place in which I draw strength from in all my accomplishments. If it were not for my wife's English and grammar skills, some of my professors might have ripped their hair out when looking over my papers throughout my Masters degree. I can never give enough thanks to my wife for all the things she has done to support my education and my career.

To Dr. Cheryl Banachowski-Fuller, she has been my advisor as well as my professor throughout my Masters degree. I thank her for her support in my long degree process, she kept me focused when it was needed, she kept my abreast of my degree goals and was very supportive of me even when I had to postpone my degree to deploy overseas multiple times.

To Stephen Cornish, friend and Attorney at Law: You are my best and oldest friend and if it were not for your constant support and competition between each other, I may not have wanted to finish my Masters degree. Since you have completed your law degree, I guess the next step is my doctorate.

Finally, this paper is dedicated to law enforcement agencies at all levels; iris recognition and biometrics in general will be an effective tool, which can be implemented at all levels of operations. I feel if iris recognition is implemented and allowed to stay within the confines of law enforcement and homeland security, it will be a powerful instrument in all of its actions.

Abstract

Expanding Biometric Operations in Law Enforcement to Include Iris Collection

Jeremiah T. Bruce

Under the Supervision of Dr. Cheryl Banachowski-Fuller

Statement of Problem

A biometric is a physical or biological feature or attribute that can be measured. Biometric collection is not a new science to law enforcement, with the collection of fingerprints dating back to the 1800s. As biometric collection technology progresses and new technologies are discovered, the expansion of biometric collection would be a great tool for law enforcement agencies. Current biometric technologies can collect a number of modalities ranging from fingerprints, facial picture, iris scans, retinal scans, to measuring gait, palm geometry and DNA sequencing. By using some of these new technologies, such as iris recognition technology, can add a new dynamic to law enforcement operations by taking a more efficient and less invasive approach towards biometrics collection. In the realm of law enforcement, biometric technologies would assist in corpse identification, criminal investigations, parenthood determination and missing children cases (Ross et al., 2006).

Although some law enforcement organizations are starting to use biometric collection, one overall system has yet to be used which limits overall capability. There is general agreement in the biometrics world that significant questions remain in the areas of performance, scalability, and security of biometric systems especially when applied to an ever-increasing number of users as currently envisaged in national and international programs (Ratha, 2008). Using iris recognition technology has proven to be an effective tool in border security in places such as United Arab Emirates (Vacca, 2008). By adopting iris recognition collection within law enforcement agencies, they will be using a technology that does not have the 'criminal' stigma of fingerprint collection and a system that is far more efficient in regards to database searches (DGJRC, 2005). No police agencies are currently using iris recognition technology as part of its daily operations (Krishnan, 2004), although it is being utilized within the criminal justice system, in limited capacity, with a few correctional facilities (Woods & McLaughlin, 2006).

Methods of Approach

In using secondary data, a review of biometric programs will show the need for the expansion of the use of biometric technologies by law enforcement. Observations and professional experience with biometric systems and their deployment will be summarized to show the effectiveness of biometric systems in operational settings. Information from foreign research agencies and data from accredited journals and sites to include the US Department of Justice and Defense will be presented. Conclusions and recommendations to expand the use of iris recognition systems will be based on collective information presented.

Results of the Study

The information contained in this study supports the expansion of biometric collection by law enforcement agencies to include iris recognition. Iris recognition technology shows the iris as a very distinctive biometric, more distinctive than fingerprints or DNA. The noninvasive manner in which irises are scanned and processed are very efficient even in databases with millions of irises. Iris recognition presents an effective tool to local, state and federal law enforcement agencies to identify individuals for both criminal and homeland security activities.

TABLE OF CONTENTS

SECTION I: INTRODUCTION

Expanding Biometric Operations in Law Enforcement to Include Iris Collection

A biometric is a physical or biological feature or attribute that can be measured. Biometric collection is not a new science to law enforcement, with the collection of fingerprints dating back to the 1800s. As biometric collection technology progresses and new technologies are discovered, the expansion of biometric collection would be effective advanced tool for law enforcement agencies (Vacca, 2007). Current biometric technologies can collect a number of modalities ranging from fingerprints, facial picture, iris scans, retinal scans, to measuring gait, palm geometry and DNA sequencing. By using some of these new technologies, such as iris scan/recognition technology, they can add a new dynamic to law enforcement operations by taking a more efficient and less invasive approach towards biometrics collection. In the realm of law enforcement, biometric technologies would assist in corpse identification, criminal investigations, parenthood determination and missing children cases (Ross et. al, 2006).

The large number of agencies involved in the homeland security and law enforcement fields require biometric devices that meet established standards and that improve interoperability and access to biometrics data across user communities (NSTC, 2006). There is general agreement in the biometrics world that significant questions remain in the areas of performance, scalability, and security of biometric systems especially when applied to an ever-increasing number of users as currently envisaged in national and international programs (Ratha & Govindaraju, 2008). Using iris recognition technology has proven to be an effective tool in border security in places such as United Arab Emirates (Vacca, 2007). By adopting iris recognition collection within law enforcement agencies, they will be using a technology that does not have the ‘criminal’ stigma of fingerprint collection and a system that is far more

efficient in regards to database searches (DGJRC, 2005). If a biometric collection standard can be agreed upon, using technology such as iris recognition, agencies can then collaborate too efficiently and effectively implement common biometric tools for use across geographic and departmental goals (NSTC, 2006).

The significance of this research is to address how advances in biometric technology, particularly iris recognition will change the methods law enforcement agencies use in conducting daily operations. By using the tools iris recognition provides, law enforcement agencies can better protect its populace and borders (Vacca, 2007). In addition, although a loss of civil liberties and privacy is one of the main concerns of the general population (DGJRC, 2005), this research suggest that the use of iris technologies and biometrics from law enforcement agencies does not have to be an infringement on citizen rights.

As of yet, the expanded use of biometric technologies by law enforcement agencies have not ventured much beyond fingerprint recognition. According to industry analysts, worldwide biometric industry revenue is expected to soar from $2.6 billion to $6.4 billion in 2011, with government and law enforcement account for almost half of total (Vacca, 2007). With new technologies, it is easy to predict the court system will have difficulty in accepting the new practices in law enforcement. This will be further mitigated as law enforcement agencies elect the use of independent biometric collection systems which could affect the way information is collected and shared in between agencies (DGJRC, 2005). With iris recognition it provides a singular technology, that is fast and efficient and is one of the most unique and accurate biometric modalities (Daugman, 2003).

Biometric characteristics can be considered as a bridge between an identity record and the individual the record belongs to. Public acceptance of the use of new biometrics

technologies is also a difficult task for individuals to grasp. Fingerprints have been used since the 19th century, and more recent DNA analysis has become routine in assisting criminal investigations. It is due to this history that many citizens associate enrollment in biometric systems with criminals and hence tend to resent it (DGJRC, 2005). Iris recognition does not have the same stigma and with advances in iris capturing technology, an iris can be collected in about the same amount of time a normal picture is taken (Daugman, 2007).

In using secondary data, a review of biometric programs will show the need for the expansion of the use of biometric technologies, particularly iris recognition technology, by law enforcement. Observations and professional experience with biometric systems and their deployment will be summarized to show the effectiveness of biometric systems in operational settings. Information from foreign research agencies and data from accredited journals and sites to include the US Department of Justice and Defense will be presented. Conclusions and recommendations to expand the use of iris recognition systems will be based on collective information presented.

This research will serve as tool for law enforcement agencies for guidance in expanding the use of biometric systems in law enforcement related to iris recognition technologies. Specifically, the expanded use of iris recognition technology will show law enforcement policy makers and administrators the effectiveness of biometric systems in daily operations and the use of biometric systems in protecting national borders. Overall, a general understanding of the expanded use of biometric technologies, particularly iris recognition, will be relayed in the content of this research.

SECTION II: LITERATURE REVIEW

Introduction

This section is divided into four parts. Although collecting biometrics is not a new science, many of the types of biometrics being collected nowadays are new. To properly define some of the new terms and techniques, this section is divided into specific terms used in biometric collection, types of biometric modalities, types of systems and the functionality and cost of these systems. Terms were derived from a multitude of sources but the terms are generally accepted by both national and foreign entities.

Specific definitions of biometric terms

In defining biometrics in the simplest of terms, shows 'bio' meaning life and 'metrics' meaning measurement, therefore biometrics is the measurement of life. In more advanced terms, biometrics can be described as both a characteristic and a process. Biometrics as a characteristic is a measurable physiological and behavioral characteristic that can be used for automated recognition (Krishnen, 2004). As a process, biometrics is the automated methods of recognizing an individual based on measurable physiological and behavioral characteristics. Physiological biometrics measures the distinct traits people have, usually (but not always or entirely) dictated by their genetics (BTF, Aug 2008). Examples of physiological biometrics include advanced techniques like DNA, voice pattern, retinal scans, iris scans and facial geometry, but also well-known methods like fingerprinting and photography. A behavioral biometric is a characteristic learned and acquired over time rather than one based primarily on biology. (BTF, Aug 2008). Examples of behavioral biometrics include voice printing and gait analysis, which use computers to analyze the sound created by the human voice box or the movement of a person walking. A more common behavioral biometric is the handwritten signature, used daily by people to

formally or informally signify their authorship of a document or assent to an agreement. It should be noted voice pattern is both a physiological and behavioral trait depending on what specific aspect of the voice pattern is being observed. A variety of automated computer systems record collected biometrics and can then be used to identify individuals already in the system (Vacca, 2007).

When using biometrics the generic term recognition is often used. Recognition is used in the description of biometric systems (i.e. face or iris recognition) relating to their fundamental function, recognition does not inherently imply verification or identification (NSTC, Sep 2008). A biometric is collected and compared to all the reference information in a database, depending on the reason why the biometric was collected, a verification or identification occurs. Verification is the task where the biometric system attempts to confirm an individual's claimed identity (a one to one matching process), but comparing a submitted sample to a one or more previously enrolled biometric (Asking: Am I who I claim to be?) (NSTC, Aug 2006). For example, if a company is using a biometric system as an access roster for the building, when an employee tries to gain access to the building the biometric system is verifying the employee is in the biometric database. Identification is the task which the biometric system searches a databases for a reference sample and if found, returns a corresponding identity (NSTC, Aug 2006). The biometric system performs a one to many matching process (Asking: Who am I?). There are two primary categories for identification: closed set and open set identification. Closed-set identification is a task where an unidentified biometric subject is known to be in the database and the system attempts to determine his/her identity (BTF, Aug 2008). An open-set identification is a task that more closely follows operational biometric system conditions to 1) determine if a biometric subject is in a database and 2) find the record of the biometric subject in

the database. This is sometimes referred to as the 'watchlist' task to differentiate it from the more commonly referenced closed-set identification (BTF, Aug 2008). Verification and identification are related processes; with the only major difference being identification is used to determine whether or not a person is known, this can be valuable information, particularly in situations where an organization cannot or for various reasons chooses not to ask the individual to identify him or herself (NSTC, Sep 2006).

Biometrics cannot singlehandedly solve all the problems with identifying individuals within the realm of law enforcement (Rosen, 2004). While biometrics serves as just one tool in a very large identity management toolbox, it is the most definitive real-time tool currently available (NSTC, Aug 2006). Several aspects must be addressed when collecting biometrics and the maintaining of a biometric database: Identity management is the combination of systems, rules and procedures that defines the agreement between an individual and organizations regarding ownership, utilization and safeguard of personal information (DoD, Nov 2006). Identity governance is the combination of policies and action taken to ensure enterprise-wide consistency, privacy protection and appropriate interoperability between individual identity management systems. Derived from these terms comes the goal of any biometric system, Identity dominance (DoD, Nov 2006). Identity dominance is a broad discipline that deals with establishing the true identity of individuals in a system (such as a country, a computer network, or an enterprise) via the use of biometric signatures, and subsequently establishing a knowledge base associated with that identity via intelligence exploitation, production, and dissemination of identity information (DoD, Nov 2006). The identity dominance process includes: biometrics collection, transmission, matching and storage, intelligence analysis and production (including intelligence forensics), dissemination to or action by consumers. This is accomplished through

the use of enabling technologies and processes to establish the identity of an individual and to establish a knowledge base for that identity (BTF, Sep 2008).

Types of modalities

There are many biometric systems currently in use in both the private and public sectors. Systems can collect one or several biometric types or modalities. Most individuals should understand individual modalities, but might not understand biometrics as a whole. It goes without saying; most individuals have seen biometrics in use, such as fingerprint collection at a crime scene on a television drama (although often times inaccurate in their depiction). There is a great multitude of modalities; despite when you think how genetically similar humans are to one another (NSTC, Sep 2006). Whether or not an individual directly relates modalities to biometric collection or biometric systems, many individuals will recognize the modalities. There is no single biometric modality that is best for all implementations (NSTC, Sep 2006).

Physiological biometrics:

Iris recognition relies on capturing the image of the color part of an individual's eye. The iris, which is actually a muscle, controls the pupil of the eye and regulates the amount of light that is allowed to enter the eye. An iris scan is a high-quality photograph of the iris taken under near-infrared (near-IR) illumination (Daugman, Jan 2004). Though visible light can also be used to illuminate the eye, individuals with dark pigmented eyes reveal more reference points under near-IR light. The resulting photograph is analyzed using algorithms to locate the iris and extract feature information, in order to create a biometrics template or 'IrisCode', the patented iris recognition code/algorithm issued to John Daugman (Daugman, 2003).

Facial recognition is the most common and recognizable biometric. Most forms of identification require a facial photo, and we, as humans, are basically facial recognition systems,

since our faces is how we generally differentiate between one another. Facial recognition systems attempts to identify a subject based on eye socket position, space between the cheekbones, position of the nose, etc…

Fingerprint recognition is one of the most well-known and publicized biometrics (NSTC, Aug 2006). Fingerprint recognition systems rely on the biometrics device's ability to distinguish the unique impressions of ridges and valleys made by an individual's finger. It is scientifically proven that fingerprints do not repeat themselves between individuals, even when considering identical siblings. An individual can be convicted in a US court of law off of one fingerprint, and as stated before the Federal Bureau of Investigation (FBI) Integrated Automated Fingerprint Identification System (IAFIS) has over 50 million sets of fingerprints in its database (Vacca, 2007).

Retina recognition uses the patterns of blood vessels on the thin nerve on the back of the eyeball that processes light entering through the pupil. Retina recognition can be confused with iris recognition since it is viewed as taking a biometric of the eye. The two recognition systems look at two different aspects of the eye, but retina scans often require individuals to remain still for 30-60 seconds as the device records the retina, and requires the scanner to be placed within an inch of an individual's eye. Whereas iris scanners can capture an individual's biometric from a foot or more away.

Hand geometry recognition uses dimensional measurements to record an accurate spatial representation of an individual's hand. Hand geometry has become very popular because of the ease of use, public acceptance and integration capabilities (NSTC, Sep 2006).

Voice recognition simply uses an individual's voice for verification or identification. There are two forms of voice recognition: Text dependent, which requires the individual to speak a

prepared statement that is programmed into the systems. Text independent is described as the biometric system having no advanced knowledge of the content in the individual's speech. Behavior biometric aspects of voice recognition would include stress patterns in the individual voice to identify the individual.

DNA recognition is another well known biometric but is the most invasive to collect. While most biometrics can be collected with little to no physical contact, DNA requires a physical sample to be taken from the individual. DNA can be collected from a number of sources (blood, salvia, hair, semen or tissue), which will all give the same result (Vacca, 2007).

Other physiological biometrics includes but are not limited to, body odor, brain-wave patterns, ear shape, footprint, gait, skin luminescence and vein patterns.

Behavioral biometrics:

Dynamic signature recognition measures the speed and pressure an individual uses when signing their name, not what the signature itself looks like. The way a persons signs their name is known to be a characteristic of that individual (Lee et al, 1996). Common characteristics include the velocity, acceleration, timing, pressure and the direction of the signature stokes across the X, Y and Z axes of an individual's signature (NSTC, Sep 2006).

Single and multiple modality systems

Single modality systems are biometric collection systems that conduct biometric searches off of one biometric modality (additional modalities can be collected just not searched off of). One of the biggest examples is the FBI's IAFIS system, which has over 50 million sets of fingerprints to search off (Vacca, 2007). The Combined DNA Index System better known as CODIS allows law enforcement and government agencies to conduct biometric comparisons and produce biographic profiles using DNA. Other examples include the Tampa Police Department use of

FaceIt ™, at the 2000 Superbowl in Tampa, Florida, and other facial recognition programs such as EyeDetentity ™.

Multiple modality systems are biometric collection systems that conduct biometric searches off of the multiple biometrics the system collects. One of the biggest example of a multiple biometric system is the Biometric Automated Toolset commonly known as BAT and the Handheld Interagency Identity Detection Equipment (HIIDE), used by the United States Military in its Global War on Terrorism in Afghanistan, Bosnia, Horn of Africa, and the Middle East. The BAT system collects and searches off of three biometric modalities: facial, fingerprint and iris recognition (BTF, 2008). Other multimodal biometric systems include British Telecom Laboratories – Digital Audio-Visual Integrated Database (BT-DAVID) that collects and searches from visual and audio modalities and BIOMET multimodal database that collects face, voice, fingerprint, hand geometry and online-dynamic signature (Ross et al, 2006).

Functionality

To truly assess a biometric systems an understanding of the components, functional architecture and assessment criteria is needed. Although systems can greatly vary in the biometric modalities collected, the purpose of the collection system, or the way the information is queried, there is a fundamental basis in every system.

Typical biometric systems are comprised of five integrated components. These components make up the functional architecture of biometric systems. The component comparisons remain the same if the systems are single or multiple modalities. The components consist of algorithm creation, quality control, data storage, matching biometrics and finally the decision process (NTSC, Sep 2006).

The first component of biometric systems is they will have a sensor or sensors (biometric collection device…i.e. camera, fingerprint reader, etc.) that observes/captures biometric characteristics and converts the observations into data that can be stored in electronic form. When biometrics is collected, the converted data into electronic form is called an algorithm. The algorithm is a limited sequence of instructions or steps telling a computer system how to solve a particular problem. The algorithm is what the systems use to convert the biometric into a template, breaking down the biometric into terms the system can interpret. In layman's terms the algorithm is what the system sees instead of the actual biometric. For example, a fingerprint analyst conducts a comparison between fingerprints looking for similarities between the actual fingerprint images and the collected fingerprints: looking for minutiae details. The algorithm converts the minutiae details into the biometric template, which is stored and searched by the biometric system.

The second component is the signal processing algorithms performing quality control activities on the collected data and develops biometric templates. The biometric templates are the graphical representation reduced into a numerical/mathematical representation. The template is used by the biometric system as an efficient method to make comparisons within the system. Templates are usually a proprietary mathematical representation of biometric data that represents the biometric measurement of an enrollee (Vacca, 2007). The quality control aspect biometric systems ensure the correct template is created when the biometric is taken. For example SecureMetrics ™ Pier Iris Scanners capture three iris images and compares them to one another before creating the iris biometric template, which then the biometric system uses for biometric data storage and searches. If the templates do not match the iris scanner rejects the biometric collection and requires the collector to take another biometric. Another example is when

fingerprint readers collect fingerprints similar to the FBI 10 fingerprint card, where 10 rolled fingerprints and four finger/thumb slap fingerprints are taken. The fingerprint reader takes an additional step and makes comparisons between the rolled prints and slap prints to ensure the fingerprints match. This comparison ensures that quality fingerprints were taken with the fingerprint reader.

The third component is how the biometric system conducts data storage. This includes the management of the data collected concerning everything from initial collection to all future collections. Other areas include where the biometric information is stored, be it on an individual system or multiple systems. Last, if the data is transmitted across a closed or open network and how the information is transmitted is also addressed.

The fourth component consists of a matching algorithm that compares the new biometric template to one or more templates that may already be stored. A match is a decision that a biometric sample and a stored template comes from the same human source, based on their high level of similarity (Vacca, 2007). Based on the efficiency of the matching algorithm, biometric systems are rated in two ways: false-accept rate and false-reject rate. False-accept rate is when a biometric subject is incorrectly matched to another biometric subject's existing biometric. False-reject rate is the failure of the biometric system to identify a biometric subject or to verify the legitimate claimed identity of a biometric subject.

The fifth component is a decision process that uses the results from the matching component to make a system-level decision. This step verifies whether the biometrics submitted is actually in the biometric system. Depending on the purpose of the biometric system, verification or identification is achieved. The decision process is either automated or human-assisted (NSTC, Aug 2006). For example with BAT, when the system reaches the decision

component the system gives a full comparison on potential matches the system found. These results are ranked from a highest possible match to the lowest possible match by the system, but the final step is still decided by the human user of the BAT.

With the increased deployment of biometric-based authentication solutions in several civilian and government applications, there is a definite need for standardization of biometric systems in order (a) to facilitate interoperability between vendors, and (b) to ensure that biometric sub-systems can be easily integrated into a variety of applications. To this end, there have been concerted efforts to draft biometric standards (Ross et al., 2006). Although there are no official standard criteria for assessing biometric systems, there is a general accepted criterion on individual biometrics known as the Seven Pillars of Biometric Wisdom (Jain et al., 1999). The Institute for Prospective Technological Studies (IPTS) used the Seven Pillars of Biometric Wisdom when they conducted a biometric technical assessment for the European Parliament Committee on Citizens' Freedoms and Rights, Justice and Home Affairs (DGJRC, 2005). The 2005 study highlights a number of key issues to be taken into account when considering the large-scale implementation of biometric technologies within the European Commission. The seven pillars of biometric wisdom are as follows:

Universality of a biometric is the system's ability to collect a particular biometric, such as finger, iris, face or DNA, which can be used for identification.

Distinctiveness is how unique the biometric characteristic is for each person, and thus constitutes the biometric as a distinguishing feature.

Permanence is the basis on the collected biometric will remain largely unchanged throughout the person's life.

Collectability is ease of collecting the particular biometric in a reasonable fashion for quick identification.

Performance is the degree of accuracy of identification for the system; performance must be high for a system to be operational.

Acceptability is the public perception of the biometric collected. Regardless of the how well the biometric is collected a system could be denied if the public offers strong resistance to a system.

Resistance to Circumvention is a necessary pillar, in order to provide added security; a system needs to be harder to circumvent than existing identity management systems. Assessments are also made on the ability to spoof the system. Spoofing is the ability to fool a biometric system into recognizing an illegitimate biometric subject as a legitimate biometric subject or into missing an identification of someone in the database.

Using the seven pillars there are several examples of how the pillars are implemented:

Using the iris as a collectable biometric is probably not well known by many individuals. When compared to individuals, people see many people with blue, green, brown, etc… colored eyes. It is not shown in popular television shows that an iris scan was taken; it is always something along the lines of DNA or fingerprints that catches the criminal. The complexity and stability of the human iris pattern makes it well suited for the task of biometric verification (Ratha & Govindaraju, 2008). The universality of the iris is high; all humans (including blind people) possess irises. Exceptions include people with aniridia (absence of an iris) or other diseases that causes the pupil of the eye to become ruptured, causing a misshapen iris. Iris patterns are scientifically proven to be distinct. The iris of the eye becomes permanent during infancy and remains the same to old age. The distinctiveness of irises used in recognition software are both highly complex and unique, the chance of two irises being identical is

estimated at 1-in-10^{78}, making irises very well-suited for biometrics identification (Daugman, 2004). Collectability of irises is relatively easy to obtain but may require several attempts. The iris biometric templates offer excellent performance even identification in large databases. The acceptability of iris recognition is relatively low, although it is considered the most accurate biometric modality collected by the US Military (DoD, Nov 2006). Newer iris recognition systems are relatively difficult to circumvent (DGJRC, 2005).

Fingerprints verification has a good balance related to the seven pillars of biometrics. Nearly every human being possesses fingerprints with the exception of hand related disabilities (such as work related, missing hands or arthritis). Fingerprints are proven to be distinctive and the details are permanent. Live-scan fingerprint readers can capture high quality images. Fingerprints have a stigma of criminality associated with them but that is changing with the increased demand of automatic recognition and authentication in a digitally interconnected society. Also it is estimated that approximately five percent of people would not be able to register and deliver a readable fingerprint. This is significant when implementing large-scale applications of millions of people. By combining the use of multiple fingers, cryptographic techniques and liveliness detection, fingerprint systems are becoming quite difficult to circumvent (DGJRC, 2005).

DNA verification is a technique with a high degree of accuracy. The statistical sampling shows a 1-in-6 billion chance of two people having the same profile. DNA is present in all human beings and with the exception of monozygotic twins, it is the most distinct biometric identifier available for human beings. DNA does not change throughout a person's life; therefore the permanence of DNA is incontestable. It performs well for the applications where it is currently used (forensics, paternity tests, etc.) though it would not be suitable for every

application. DNA tests are difficult to circumvent under certain conditions (supervised sample collection with no possibility of data contamination) (Vacca, 2007). If sample is not supervised however, an imposter could submit anybody's DNA. We all leave DNA traces wherever we go (a single hair can provide a sample) and so it is impossible to keep DNA samples private (DGJRC, 2005).

As shown, the seven pillars can apply to any biometric taken. Aspects to look at are when technology changes, new equipment is created or public perceptions change, the interpretation of the seven pillars will change. Also the fact that all the pillars are subjective, what is considered to be quick in collectability to one individual may not be fast enough for another, the same would go for arguments against each of the pillars. For example using the Bertillon System, at its inception, it was believed to be an identification system that could positively identify an individual and that identification would be specific to just one individual (Jain et al, 1999). After the Will West/William West incident, is the biometric collected, using the Bertillon System, still distinctive enough now that there is a confirmed case of two individuals having the same biometric set? What would happen if two individuals were found to having matching fingerprints?

This section provides the reader with a basis in which to understand biometric terms and modalities, in an effort to show why the expansion of biometric collection, particularly iris collection, needs to occur within law enforcement agencies. Although the use of biometrics, such as DNA and fingerprints, is not new to law enforcement, there are many biometrics that are not currently collected, which are just as unique if not more (such as iris recognition) than current systems used (DGJRC, 2005). The overall functionality shows that the effectiveness of biometric systems is limited by their collection capability. Single modality systems are rendered

ineffective if the single biometric cannot be collected from the individual (missing hands, irises, etc…). Multiple modality systems collect multiple biometrics, but if an individual cannot provide a particular biometric the system can still operate while missing one or more of the biometric modalities (Ross et al, 2006). Iris collection offers a new, less invasive way to collect biometrics from an individual, which is far more accurate than current systems in use by law enforcement. The expanded use of iris recognition technology will show law enforcement policy makers and administrators the effectiveness of biometric systems in daily operations and the use of biometric systems in protecting national borders.

SECTION III: ACCEPTANCE AND REJECTION REASONING

Introduction

This section is divided into two parts. The use of biometrics in one form or another has been utilized and accepted for thousands of years throughout the world. In regards to using irises as a viable biometric acceptance of irises has not entered into the mainstream United States, with the exception of the United States Military. There are many arguments on using more types of biometric collection by law enforcement agencies ranging from increase security against terrorist attacks to a complete invasion of privacy. This section shows the arguments both for and against biometric collection within law enforcement and other entities. Since iris collection is not a widely used biometric in the United States, many examples come from different countries.

Commercial and Private Sector Acceptance of Iris Recognition

Commercial acceptance of biometrics has a surprisingly long history dating back almost 10,000 years. Businessmen in Babylon were required to give a clay handprint which would identify merchants to dealers who may not be familiar with them. Dating even farther back to 7,000 to 6,000 BC Chinese pottery makers identified their work by placing their thumb print on the pottery rather than a signature (Vacca, 2007). Evidence also shows fingerprints were used as a person's mark as early as 500 BC and according to the International Institute of Hand Analysis, "Babylonian business transactions were recorded in clay tablets that included fingerprints," (Neumann, 2007). Joao de Barros, a Spanish explorer and writer, noted early Chinese merchants used fingerprints to settle business transactions. With a very long history, why has biometrics not become more mainstream in the world?

In recent years, commercial use of biometrics has significantly increased its use of biometrics but it has not caught on universally. For computer network administrators, biometrics

replacing remembered passwords alleviates the need for users to remember their passwords, since you do not have to remember your biometrics, solving one of the network administrators' most common problems (Vacca, 2007). Corporate security has also been increased with the use of Key Fob Tokens, such as RSA SecurID ®, that produce a random number use when the user needs to gain access to the company's systems. The user is required to remember their user name and a password, but the key fob gives an extra layer of protection, and is usually considered a sensitive item, which is reported to the company upon its loss. This type of security profile eliminates key logger computer hacker programs using dynamic signature biometrics to retrieve passwords from unknowing computer users.

Iris recognition technology usage has taken a huge jump in recent years within the commercial sector. One of the largest and longest deployments of iris recognition systems is deployed at all 17 ports of entry (air, land and sea) of the United Arab Emirates (UAE). Immigration control checks all incoming passengers against an enrolled database of individuals who were expelled from the UAE (DGJRC, 2005). In its first three years of deployment and with an average of 6,500 passengers entering every day (totaling 2.1 million passenger, with 9,500 individuals being identified on the 'do not enter' list), the system has been described as very fast and effective (Daugman & Malhas, 2004). The same system has been used in several European countries as a 'positive application' instead of a 'do not enter' list, in Schiphol Privium, Netherlands, Frankfurt Airport, Germany, and several Canadian and United Kingdom Airports (DGJRC, 2005; IBG, 2009). The purpose of the 'positive application' is to allow individuals to provide their biometrics (particularly irises) in order to use a faster line in security checks at the participating airports. During the 1998 Winter Olympic Games, iris recognition was used to check out rifles for the biathlon (Woodward et al, 2001).

Financial institutions have also attempted to use biometrics as a way to bring new security to banking. Bank United of Texas was the first bank in the United States to implement iris recognition at Automated Teller Machines (ATM) and the first bank to use the technology of a single factor mode, within Personal Identification Numbers, passwords or cards, but by using an IrisCode record (IBG, 2009). A similar pilot iris ATM program was also conducted by Nationwide Building Society, a British saving and loan institution. In a Washington Post article (1999), showed the initial results of the customer polls showing 94% of individuals were comfortable with the system and 91% preferred using their irises instead of a PIN or Signature (Gugliotta, 1999).

The private sector has an even greater acceptance of biometrics than of the commercial sector. The collection of biometrics dates back 31,000 years with the discovery of handprints of prehistoric men who lived in caves. The walls of the caves were adorned with paintings and surrounding these paintings were numerous handprints that are felt to "have . . . acted as an un-forgeable signature" of its originator (Neumann, 2007). Chinese parents also used fingerprints and footprints to differentiate children from one another (Vacca, 2007). In regards to current technology, individuals have seen or used a multitude of devices allowing the user to access their personal devices, such as laptop and desktop computers, portable storage devices and even biometric access to an individual's home. The iris recognition software allows you to attach the device to your computer and use it to gain access to a system or door but its overall cost is high and the technology deployment can lock the user into a particular device or brand making iris recognition systems not very functional for private use (DGJRC, 2005).

Government Acceptance of Iris Recognition

Government agencies have recently started or have been using iris recognition in a number of different capacities. On the smaller scale iris recognition technology has been fielded in public schools. One particular class was in New Egypt, New Jersey, school staff and administrators were placed into a biometrics database and the only way to gain access into the school was to scan their irises to have the door unlock (Cohn, 2006). Venerable Bede School in the United Kingdom has also implemented a similar iris recognition system to be utilized in the library to check out materials and to make purchases at the cafeteria (IBG, 2009). Several airports, Logan International Airport, MA, and John F. Kennedy Airport, NY, have also implemented iris recognition systems for physical access into restricted areas of the airport (IBG, 2009). Pakistan has also used iris recognition in conjunction with United Nations High Commissioner for Refugees (UNHCR) in Pakistan to track refugees seeking assistance to return to Afghanistan (UNHCR, 2003; Vacca, 2007). The system is used to detect anyone who has been previously enrolled in the database and is seeking assistance (a one-time cash grant from the United Nations) for a second time. All of these functions have a specific goal and the information collected is not utilized for anything other than what it is originally intended (UNHCR, 2007).

The Department of Defense has used biometrics in its military operations for many years. The current systems in widespread use are the BAT and the HIIDE; both systems utilize iris recognition along with fingerprint and facial recognition (BTF, 2008). With the BAT and the HIIDE the Department of Defense is able to make a Biometrically-Enabled Watchlist (BEWL) (DoD, November 2006). A BEWL is any list of person of interests, with individuals identified by biometric sample instead of by name, and the desired/recommended disposition instructions

for each individual (BTF, 2008). Using the biometric collection devices allows for identity dominance which is the operational capability to achieve an advantage over an adversary by denying him the ability to mask his identity or to counter our biometric technologies and processes. This is accomplished through the use of enabling technologies and processes to establish the identity of a biometric subject and to establish a knowledge base for that identity. This includes denying an adversary the ability to discover our protected assets (BTF, 2008).

One of the earliest adopters of biometric technology has been law enforcement, there is a rich history of using biometric identifiers to recognize prisoners and repeat malefactors (Woods & McLaughlin, 2006). In regards to iris recognition systems, there are two particular case studies which has used iris recognition technology to further secure it facilities Jefferson County Jail and the Contra Costa County Office of the Sheriff. In the Jefferson County Jail, officers utilized a Pier Iris Recognition device to track individual prisons to ensure they were positively identified and placed in the correct facilities and given access to areas in which they were permitted (Woods & McLaughlin, 2006). The Office of the Sheriff in Contra Costa County used the Omni Jail Management System to positively identify individuals from prisoner intake to release (L-1, 2009). Beyond cost, iris recognition systems are preferred over other biometric modalities systems due to the fact that irises are considered the most accurate biometric (beyond DNA and fingerprints) and one of the most non-invasive when it comes to collection (Daugman, June 2004; Woods & McLaughlin, 2006; Vacca, 2007). Under the Patriot Act and the Enhanced Border Security and Visa entry Reform Act, the Department of Homeland Security and Department of State began using the U.S. Visitor & Immigrant Status Indicator Technology (US-VISIT) Program to check fingerprints of foreigners entering the United States (Vacca, 2007). US-VISIT is one of the largest biometric collection efforts by a law enforcement entity, which

works as border security system that has been deployed at 115 airports, 15 seaports and in secondary inspection areas of the 50 busiest land ports of entry (Ross et. al, 2006). The US-VISIT system collects both right and left thumb prints of a foreign visitor to validate an individual's travel documents at the port of entry. Although this is a rather large collection effort, the standard collection of two thumb prints is not compatible with the FBI's IAFIS. The most well known biometric system is the FBI's IAFIS, which 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. AFIS is predominantly used for law enforcement, but is also being used for civilian applications and security clearance background checks (BTF, 2008). Even with the widespread acceptance of biometrics and iris recognition, other than the few iris recognition examples (shown above), iris collection is not in mainstream usage within the United States.

Rejection Reasoning

There are many reasons why individuals in the United States and the world would reject the ideal of having their biometrics taken with one of the main reasons being an invasion of privacy. In the United States, privacy has a great deal of value for our society and culture, and this importance is reflected in our laws (Woodward et al., 2001). Concerns on collecting biometrics can fall into three main categories; information privacy, physical privacy and religious objections. Other concerns are related to cost and overall functionality of a biometrics system being deployed in a country as large as the United States.

Information privacy concerns within biometrics, function creep means biometric data originally collected for one purpose are used for other purposes (Woodward et al., 2001). Examples of function creep with biometrics and other types of identification programs have been

seen throughout the world. One of the largest biometric systems in the world is a facial recognition system in the United Kingdom. The system is being used in conjunction with an estimated four million cameras (some estimates are much higher) located at prominent streets and thoroughfares, continually scanning pedestrians to find fugitives and terrorists (Vacca, 2007 & Rosen, 2004). Although the cameras in United Kingdom were initially justified as a way of combating terrorism, they soon came to serve very different functions: Seven hundred cameras now record the license plate number of ever car that enters central London during peak hours, to confirm drivers have paid a five-British Pounds traffic-abatement tax (Nock, 1993). Another example of function creep is utilizing the Face-It ™ technology on the faces of thousands of fans entering the Super Bowl in Tampa, FL, in 2000, the matches produced were not terrorists, and they were low-level ticket scalpers and pickpockets (Rosen, 2004). Quite possible the biggest offender of function creep is the use or misuse (depending on who is addressing the topic) of Social Security Numbers (SSNs). When first devised in 1925, the SSN was issued to workers exclusively for the Social Security Administration accounting purposes, with SSN cards being issued with the phrase 'Not for Identification Purposes' (Woodward et al., 2001). In 1943, by Executive Order 9397 required all federal components/agencies use the SSN exclusively whenever the component found it advisable to set up a new identification system for individuals. The GAO (1999) submitted a report detailing government and commercial use of SSNs to a House subcommittee, the information was utilized when considering legislation regulating the use of SSNs, with the public's growing concern over identity theft (Woodward et al., 2001). In attempts to thwart function creep from commercial databases, federal laws currently restrict the personally identifiable information the government can demand from credit card and phone companies, except as part of a specific investigation (Rosen, 2004). The Fair Credit Reporting

Act limits the cases where a credit report can be disclosed to the government and the Computer Matching and Privacy Protection Act of 1988, forbids federal agencies from merging (but not accessing) databases.

The spread of biometrics and therefore the replacement of weak or no identification by a system that presents a strong identification capability may reduce the scope for privacy and anonymity of citizens (DGJRC, 2005). This leads to a specific form of function creep called tracking, where biometrics are used to monitor an individual's actions (Woodward et al, 2001). A subcategory of tracking is racial profiling, which presents additional issues to not only biometric systems but to any law enforcement activity due to violation of Fourth and Fifth Amendment rights. If a biometric database with a specific purpose, such as European airports using iris recognition systems to provide a 'fast pass' way to get through security zones, were sold as a magic wand against all threats to society, expectations are bound to be disappointed and citizens might come to feel cheats (DGJRC, 2005).

Any information derived from a biometric database and used from its original purpose presents a litany of potential problems for any individuals entered into the system. With biometrics as well as with all emerging technologies, there is a potential for abuse (Rosenzweig et al., 2004). In 1960, William Prosser surveyed roughly 300 legal cases concerning privacy issues and consolidated the various claims filed by individuals into four separate causes of action: intrusion upon an individuals private affairs; public disclosure of embarrassing private facts about the individual; publicity that places the individual in a 'false light' in the public view and appropriation of the individual's name or likeness (Allen-Castellitto & Turkington 2002). With these four separate causes of action, there are two very serious criticisms against biometric technology; biometrics are not considered secrets and biometric patterns are not revocable (Jain

et al., 2004). Basically stating biometric information is not sensitive information, which can be used to compromise systems and once the information is stolen, especially with irises, an individual cannot change their biometrics, like a person can change a password or personal identification number (PIN).

Physical privacy is another hurdle of concerns in implementing a biometric system. Concerns about stigma vary tremendously in society. In the United States, some individuals and segments of society associate fingerprinting with law enforcement, acts of criminal behavior, and oppressive government (Garfinkel, 2000; Rosen, 2004; DGJRC, 2005). Although all United States Service Members and applicants for federal employment must provide fingerprints to the FBI as part of a background check, using biometrics is nothing new (Woodward et al., 2001). The implementation of biometrics raises great privacy-related fears, such as a surveillance society or of function creep (DGJRC, 2005). Other concerns about biometric systems relates to the systems actually causing harm, such as the low intensity infrared light used to capture iris images, are primarily perceptual (IBG, 2009). The last physical privacy issue is hygiene where objections to the biometrics come from concerns about the cleanliness of sensors, much like individuals have concerns of the cleanliness of public bathrooms (Woodward et al., 2001 & Vacca, 2007). With concerns over H1N1 flu virus could only add to the concerns about implementing biometrics, although as of the date of this paper, there have been no scientific studies of evidence of biometrics systems like the US-VISIT's fingerprinting system has added to the spread of H1N1. With iris recognition systems, there is no physical contact between the collectors or the individuals being enrolled or scanned by the system (IBG, 2009 & Retica, 2009).

In particular with the United States being considered a 'melting pot' of diversity, a concern against biometric implementation is religious objections. Religious objections to biometrics might arise from a variety of different groups, for example certain Christians interpret biometrics to be a 'Mark of the Beast' (Woodward et al, 2001). Another example is the 2003 case in Florida of a Muslim female not being allowed to obtain a driver license without providing a full facial photo without the individuals using her niqab (garment meant to completely cover a woman's head with the exception of the eyes). As a result the State of Florida (Circuit Court for the Ninth Judicial Circuit, in and for Orange County, Florida, Case No. CI-02-2828, 2002) ruled against the Muslim female citing a public need to immediately identify subjects of investigative traffic stops and criminal and intelligence investigations outweigh the needs to pose for a driver's license cloaking all features except the eyes. Despite these specific cases, religious objections to biometrics are not expected to be widespread, but such objections must be taken seriously because of societal and legal emphasis on respect for sincerely held religious beliefs (Woodward et al., 2001).

Other critiques of biometric system and their deployment come down to cost and functionality. All biometric collection devices have a false acceptance rate, which this statistic is used to measure biometric performance when operating in the verification task. The percentage of times a system produces a false acceptance, which occurs when a biometric subject is incorrectly matched to another biometric subject's existing biometric sample (BTF, 2008). Bruce Schneier, a specialist on security issues, observes even with a 99.9 percent accuracy rate, the result of frequent false positives (where the system falsely identities the individual as a 'bad guy') - perhaps hundreds or thousands - at sites where there were large numbers of individuals, such as airports, will cause guards, in the end, to disregard all hits, rendering the system useless

(O'Neal, 2004). With iris recognition systems even individuals who are blind still have irises, but there will be individuals who will not be able to use the system due to certain conditions; such as aniridia or other diseases that have misshapen the iris or the pupil, drooping eyelids or long eyelashes which obstruct the iris image, the overall amount of individuals who fall into this category are relatively low (DGJRC, 2005; Daugman 2007). National-scale deployments must be inclusive as possible; hence, it is unacceptable to exclude members of outlier populations who, for various reasons, may have a nonstandard appearance or may have difficulty presenting their irises to the camera (Daugman, 2007). The cost of deploying any new biometric collection device is very costly, especially iris recognition systems, which is why skeptics say the technology is too expensive, if not foolproof (no system is 100 percent foolproof), can be hard to integrate with other systems and requires employees working the systems to change the way they work (Vacca, 2007). Other costs will include upkeep and upgrading of systems and administration costs to implement training and refresher training. The high costs of the technology deployment combined with the fear of some kind of 'lock-in' to the technological platform and the user perception of discomfort are putting the brakes on the diffusion if iris recognition (DGJRC, 2005). Although despite these hurdles, drivers such as governmental and commercial mandates to improve security and privacy, enterprise application integration and the ongoing reduction in the cost of the hardware will help overcome some of the barriers related to the widespread implementation of biometric technology (Down and Sands, 2004).

Summary

In the very near future, iris recognition technology will be deployed in ways that eliminate fraud, provide nonrepudiation of sales, authenticate funds transfer, provide signature verification, credit card authorization and access to healthcare records, intellectual property, and

much more (English et al., 2006). Based on discussions with international privacy experts and program managers, it appears biometrics, like fingerprinting, is more of an issue in other nations and cultures, and report little concern about social stigma among their populations (Woodward et al., 2001). Iris recognition and biometrics as a whole are gaining support in all areas of commercial, private, government and military entities. Biometrics can enhance almost any task to increase security and to maintain positive identification on individuals placed in the system (Vacca, 2007). Once the iris recognition patents issued to John Daugman (1993 and 1994) expired in 2004 and 2005, iris recognition has started to diffuse more rapidly (DGJRC, 2005).

There are many barriers to allowing a nationwide biometric system, albeit iris recognition or other types of biometrics systems. Each time a new technology emerges; the legal framework becomes outdated and has to be rethought according to this new reality or to set societal acceptable boundaries for it usage (Dessimoz et al., 2006). One of the aspects which can never really be addressed until it actually happens is function creep or other types of privacy violations. An iris recognition system used by department stores to identify customers (such as seen in the movie Minority Report) could eventually be merged to a criminal database to identify shoplifters entering the store. The biggest example of this is the creation of SSNs, which was originally used to identify workers are used by most government agencies and is even being used by commercial entities (such as banks, utility companies, etc...). As the machine of government becomes efficient, Congress needs to think creatively about ways of reconstructing, through law and technology, the kind of privacy protections that the inefficiencies used to guarantee [privacy] (Rosen, 2004).

SECTION IV: RECOMMENDATIONS

Introduction

This section will be divided into four parts. In this section, recommendations will be given on the expansion of iris recognition biometric collection efforts by law enforcement agencies at the local, state and federal levels. Recommendations will also include expansion in Homeland Security efforts. Privacy and civil right infringements that biometric collection efforts could produce, will be addressed. As shown throughout this research paper, studies will show the effectiveness of biometric systems in use by the international community.

Expansion of iris recognition collection by local, state and federal law enforcement agencies

As previously shown, iris recognition is considered one of the most accurate biometric modalities currently known, more accurate than fingerprints and DNA (Daugman, January 2004). As John Daugman (2003), the creator of most of the iris recognition patents, has stated, the iris is a protected, visible part of the human anatomy and the patterns are apparently unchanged during one's life, making it most useful in creating a biometrics recognition system. Iris recognition systems can be set up to act as both a close and open set, allowing for law enforcement agencies to enroll individuals that need to be enrolled, such as individuals under arrest and are being processed into the criminal justice system, and still search individuals in the general population without ever enrolling them into any database. For example, setting iris recognition systems up in an open/close-set manor, allows police officers to use an iris scanner loaded with a database of individuals with open warrants, and can scan individuals at traffic stops, checkpoints and get immediate responses, with returns in seconds (Daugman, January 2004). The reason for the quick results is the overall size of the IrisCode (512 bytes), which is created when an iris scan is taken (U.S. Patent 291 560, 1994). When making biometric

comparisons using iris recognition systems, even with databases with a total of three million irises, give returns in seconds (Daugman, 2003). These types of statistics give law enforcement agencies the ability to use iris recognition systems nationwide without bogging the individual officers and departments down with prolonged wait times. An argument can easily be risen that if a nationwide system is put into operation how much of a cost will occur if the biometric systems are set up to alert law enforcement to any individual under warrant for any reason, such as for minor offenses like failure to pay child support or bench warrants for individuals with unpaid traffic tickets (Rosen, 2004). Extraditing an individual across state lines for an unpaid parking ticket does seem excessive and it is hard to fathom any state government wanting to flip the bill for such a minor offense. Thankfully, biometric databases are set up to filter the information being loaded into devices, such as the BAT and HIIDE systems used by the US military. Using the search filters, local jurisdictions can determine what level of offense will be loaded into the iris recognition devices. An example of this filter method, would be a local enforcement agency using the nationwide database to load all individuals wanted on felony arrest warrants, regardless of which state the individuals are from, and then using the database to put all individuals with any type of warrant that are specific to the local jurisdiction's area. Another example is the State of Arizona could have an agreement with the State of California and Nevada to detain anyone with any type of arrest warrant, due to the close proximity to each other, the filters can once again make these changes. The level of filtration can be determined by state and local governments' standing operating procedures but by submitting all the biometrics into the database allows each level enforcement agency to make those determinations.

To add in the expansion of iris recognition systems into federal agencies further solidifies the power of using this biometric modality in a nationwide database. As the country and the

world become more mobile and more integrated, the need for a system such as iris recognition becomes apparent. The Department of Homeland Security facilitates several agencies that work at the federal level and in conjunction with state and local law enforcement agencies as well as with international agencies (Vacca, 2007). This in turn demands a new quality of interagency interaction for planning, implementing, and evaluating the necessary strategies (Borchert, 2006). Contemporary security challenges such as terrorism, organized crime, the proliferation of weapons of mass destruction, cyber risks, or mass migration are transnational, originate within or beyond states, and involve non-state actors that are ready to use force (Borchert, 2006). Although homeland security is an issue the United States needs to specifically address, the United States is not the only country that has issues with how to implement security procedures and determine what information is passed between countries. The issue of homeland security should be as important to Europeans as it is to Americans, the general public and politicians in most countries of the European Union (EU) have so far paid little attention. One of the main reasons of this development is the divergence of the respective risk perceptions on both sides of the Atlantic (Föhrenbach, 2006). Since biometrics, other than fingerprints, have not been collected on individuals on a federal level, privacy determinations have not been fully discussed in the United States, but in EU biometrics and biographic information (name, height, weight and other identifying information, but nothing such as national identification numbers) by themselves are not considered sensitive information (DGJRC, 2005). Using this same biometric rule the EU is using, it is possible to share biometric and biographic information the United States is tracking with international agencies, without disclosing why the United States is tracking those individuals, and vice versa. In this manor sensitive information only has to be shared on a case by case basis and promotes an overall sharing of information between countries. Today, the

largest application of fingerprint technology is the FBI's AFIS used by police forces throughout the U.S. and in over 30 foreign countries (Bowman, 2000). Only problem with fingerprint systems is the various countries utilize different fingerprint collection systems, that are not of the same quality or same format which does not promote quick results (Vacca, 2007). Even with the John Daugman patents having expired or will expire by 2011 (NSTC, August 2006), all the current systems are still utilizing the same format when they collect iris scans. The databases and user interfaces will be different but the individual IrisCodes created by the devices are all the same, allowing for biometric information to be easily passed. As previously shown, using iris recognition is very efficient in making biometric matches, which even on a world wide database scale, a small amount of time is taken to make a match, which indicates the relative easiness of implementing biometric systems with local, state and federal agencies as well as international agencies.

Quelling privacy and right infringement in the general populace

The purpose of the research was to show the possible benefits of using iris recognition, having stated that, it is hard to get past any privacy and right infringement issues that can arise. No law enforcement agency is currently using iris recognition technology in its operations (Krishnan, 2004), although it is being used by government and commercial organizations as previously shown in this paper. The thought of implementing such an action should bring up possible Fourth and Fifth Amendment violations of unreasonable searches and due process of law. Even though as previously stated, iris recognition systems can be set up to perform as a closed-set system, where it only searches its database for matches in the system, if no match is found the biometrics collected are <u>not</u> stored. How do you convince the public that law enforcement agency collecting the information is actually just checking against the database and

not actually storing any information? Also using the earlier example of loading a biometric database with nationwide warrant information, if an law enforcement officer comes across an individual in a vehicle and finds he has a warrant for his arrest in a different state, under minor drug charges, should the officer be allowed to execute a search of the person and the vehicle? Arguments could go either way stating yes, the search is allowed because the individual could be arrested since there is a warrant for the individual's arrest and no, saying it is an unreasonable search conducted on a minor offense warrant and not to mention the due process of law where the individual has yet to be convicted on the charges (innocent until proven guilty). The perceptions of Americans are going to be different than people in say United Kingdom, where the public accepts the largest closed circuit video surveillance system in the world, which does conduct facial recognition, due to its culture, history and laws (Rosen, 2004). It is difficult to accurately assess any privacy concerns Americans will have because executing an iris recognition program has not be implemented by any law enforcement agency and different law enforcements agencies are going to have different standards in which they will collect biometric information. As of the date of this paper, these concerns are mainly on a speculative level, since no implementation of iris recognition by law enforcement agencies has been conducted.

Effectiveness of biometric programs

Biometric programs have proven successful as well as unsuccessful. The United Kingdom's closed circuit surveillance system has never captured a terrorist, even though it has millions of cameras throughout the country. The facial recognition system, FaceIt ™, was utilized at the 2000 Superbowl in Miami, Florida, and the only individuals who were identified by its system were ticket scalpers and pickpockets (Rosen, 2004; Vacca, 2007).

Despite these failings or shortcomings of some biometric systems, iris recognition has proven it is an effective system, which brings rapid responses, with an uniqueness far beyond fingerprints and DNA, and has a biometric that can be used to identify most of the population (Second Pillar of Biometric Wisdom: Distinctiveness). United Arab Emirates' iris recognition program is an excellent example of the effectiveness of such systems. The program has helped its government keep over 420,000 individuals, who were expelled for various reasons, out of the country, despite the fact individuals have tried to reenter using false identification and documentation (Daugman & Malhas, 2004). If an iris recognition system is employed correctly, regardless of whom they say they are, individuals cannot fake their biometrics. To further show the efficiency of iris recognition, new devices such as Eagle Eyes (TM), allows its iris recognition system to scan, identify and track up to 40 individuals approaching its scanner at distances as far away as 10 meters with the same rapid response as most iris recognition systems (Retica, 2009). To add to the effectiveness of iris recognition programs, facial photos can be added to iris record to allow for a secondary identification. As previously stated, one of the problems with biometrics systems is a false acceptance rate, by adding photos to a record, when a match occurs the security personnel can make a judgment call on how to react. The famous 'Naked/Blob Machine' used in some airports as a security measure, which is able to scan through an individuals' clothes (essentially allowing the user to see someone naked, which is why the system now distorts images to a 'blob-like' but still see if the individuals are concealing something on their person), did not allow individuals using the system to store or print images, so after the scan is complete, the screen image is destroyed (Rosen, 2004). With iris systems being able to be both closed and open-set systems, devices such as Eagle Eyes ^{TM}, can be used to scan individuals into its system and when a match does not occur, the system deletes the scan,

allowing the same privacy concerns of the Naked/Blob Machine to be addressed. Even if the technology currently available is not considered efficient enough (accuracy had been well proven), fearing long delays at security points or, if implemented, during law enforcement activities, Moore's Law will in the end allow for the technology to eventually work. Moore's Law, simply states electronics, mainly computer systems, will double in processing power and efficiency every six months (this is why many computer buyers tend to get upset that the computers they buy are obsolete a year after purchase), a theory that has proven for the most part true since 1965 (Moore, 1965). In theory, with iris recognition systems, processing power will only increase, the distance to take iris images will only increase and with systems such as Eagle Eye(Tm) will be allowed to track more individuals. Shown throughout this paper, iris recognition systems have proven their worth in actual real world situations and the technology will only become more effective as time passes.

Summary

Iris recognition technology can allow for local, state and federal agencies to have a centralized database. As previously shown, iris recognition systems have proven that even with large databases (totaling in the millions) the systems can be setup to give returns in seconds, which allows for many law enforcement agencies to incorporate iris recognition (traffic stops, security checks, etc...) without bogging down police activities in wasted time. Privacy and civil infringement rights raises concerns on iris recognition systems, and biometric collection in general. With the ability to create a closed-set system, which takes an individual's biometrics against a known database (such as a terrorist watchlist or for law enforcement activities an open warrant list), if a match is found, the system user is alerted, if no match is found, the biometrics collected are deleted. The filter abilities of biometric database systems allow for law

enforcement agencies to regulate what information will go into its iris scanners. The database can be collected at a federal level and distributed between local, state and federal law enforcement agencies. With the effectiveness of iris systems seen in other areas of the world, the powerful tool iris recognition would grant to law enforcement agencies cannot be ignored. No empirical data exists on implementing such a system, since no police agencies are currently using iris recognition technology as part of its daily operations (Krishnan, 2004), so it is difficult to prove or disprove the effectiveness of iris recognition being utilized by a law enforcement agency.

SECTION V: SUMMARY AND CONCLUSIONS

As shown throughout this seminar paper, iris recognition systems and the technology they represent are a very accurate and efficient biometric system to use. Iris recognition has proven itself to be more distinctive than fingerprints and DNA, with the collection systems returning results in seconds even with databases with millions of irises (Daugman, 2004; DGJRC, 2005; Vacca, 2007). Being accepted commercially, in the private sector and by the United States government, to include the United States military, has shown iris recognition is an accepted use amongst the populace. The data collected by iris recognition systems, bears no resemblance to that collected for any purpose other than real-human authentication, so the technology is free of any surveillance-related or criminal/forensic stigmas (Vacca, 2007). Despite all of this evidence, no law enforcement agency has implemented iris recognition in its daily operations (Krishnan, 2004).

Even with all the benefits of iris recognition, two major concerns arise; the functionality/cost of such a system and privacy concerns. Cost is one of the most daunting problems to overcome when implementing any new system. With the complexity and size of the US, using iris recognition would become a very costly endeavor. With iris recognition, costs are coming down as the original patents on iris recognition technologies have expired (DGJRC, 2005; NSTC August 2006), allowing companies to produce new devices and systems, while lowering cost. One of the other objections to cost with iris recognition is agencies may feel a 'locked in' requirement, with the agencies depending on one manufacturer for the systems and database (DGJRC, 2005). Irises, as a collectable biometric, are considered an unique biometric but there is a small amount of the any given population who will not be able to use the system. With iris recognition systems even individuals who are blind still have irises, but there will be

individuals who will not be able to use the system due to certain conditions; such as aniridia or other diseases that have misshapen the iris or the pupil, drooping eyelids or long eyelashes which obstruct the iris image, the overall amount of individuals who fall into this category are relatively low (DGJRC, 2005; Daugman 2007). Even with these limitations, iris recognition has one of the smallest outlier populations of people who cannot give a biometric sample out of all the biometric modalities; with the exception of DNA, which everyone can provide a DNA sample (Vacca, 2007).

Privacy issues stem from three main categories; information privacy, physical privacy and religious obligations. With physical privacy, iris recognition is not invasive as far as collection is concerned; in the time its takes to capture a photo an iris scan can be captured (L-1, 2009). With religious obligations, there are a few concerns that are related specifically towards iris recognition (Woodward et. al, 2001), this may be from the lack of widespread usage or when implemented, such as port of entry operations in UAE, where gaining access to UAE requires individuals to submit to an iris scan (Daugman & Malhas, 2004). Similar requirements are presently in effect for foreign nationals going through ports of entry using the US-VISIT system, in the United States (Vacca, 2007). Out of three privacy issue categories information privacy is of the greatest, especially with function creep. If law enforcement agencies, albeit local, state or federal, were to implement an iris recognition program, what would be the limits, if any, on collection efforts and criteria? In an effort to eliminate function creep (for full definition see Section III, Rejection Reasoning), one simple conclusion can be reached; create an iris recognition program under the control of the Department of Homeland Security, for purpose of national security and law enforcement activities only. Operations such as Port of Entry would be handled by the Transportation Security Administration and by the U.S. Customs and Border

Protection. Terrorist watchlists and 'no entry' watchlists would be constructed by the Department of Homeland Security in conjunction with the Federal Bureau of Investigation and other intelligence agencies. The biometric information gathered by the federal agencies is then distributed with local and state agencies and combined with their warrant databases (as explained in the Recommendations section). The database would even extend to illegal immigrants and all agencies and organizations requiring immigration status to be verified, since U.S. Immigration and Customs Enforcement and U.S. Citizenship and Immigration Service is under the Department of Homeland Security. All information is used for homeland security and law enforcement activities, in a closed-set system, where individuals scanned with no matches (which would be the overwhelmingly majority of the population), have their scans immediately purged from the system.

The main focus of the paper is to show the possibility of using iris recognition systems within law enforcement agencies. Even with the drawn conclusion of a grand iris recognition system, under the direction of the Department of Homeland Security, one fact has to be remembered about this system, it is only a tool, which can be utilized by law enforcement agencies. As Jeffery Rosen's chapter 'Silver Bullet' in his book The Naked Crowd (2004), he stated individuals tend to rally behind a security system (such as iris recognition) and this system will singlehandedly answer all the security questions and when an terrorist event occurs, or for purposes of this paper, an individual who should have been arrested gets away, the system is considered an overall failure. If dangerous individuals cannot be identified using biometrics, then verification instruments are largely meaningless, as suspects can hide their intent, not their identities (O'Neal, 2004). If a iris recognition system were to be implemented at a local, state or national level, the law enforcement agencies using the system still have to do their jobs, the

system only offers a way to identify individuals who are known in the system, which can encompass databases at the local, national and potentially international level, in a very efficient and precise manner. The purpose of biometric systems, albeit iris recognition or the number of other types of biometric systems currently in circulation, is to identify individuals in its respective system(s) and to take away the ability for an individual to hide their identity, nothing more, nothing less.

REFERENCES

Allen-Castellitto, A.L. & Turkington, R.C. (2002). Privacy Law: Cases and Materials. Thompson West.

Borchert, H. (2006). Homeland Security and Transformation: Why It Is Essential to Bring Together Both Agendas. In E. Brimmer (Eds,). Transforming Homeland Security: U.S. and European Approaches (pp. 3-22). Washington, DC: Center for Transatlantic Relations, 2006.

Bowman, E. (2000). Everything You Need to Know About Biometrics. Identix Corporaition.

Cohn, J.P. (July 2006) Keeping an Eye on School Security: The Iris Recognition Project in New Jersey Schools. NIJ Journal, No. 254.

Daugman, J. (2003) "The importance of being random: Statistical principles of iris recognition." Pattern Recognition, No. 36.

Daugman, J.(January 2004) How Iris Recognition works. IEEE Transactions on Circuits and Systems for Video Technology, Vol. 14, No. 1.

Daugman, J. (June 2004) BIOSEC conference. Barcelona, June 2004. University of Cambridge, England.

Daugman J (2007) "New methods in iris recognition." IEEE Transactions. Systems, Man, Cybernetics.

Daugman, J. & Malhas, I. (2004). Iris Recognition Border-Crossing System in the UAE. International Airport Review, Issue 2, 2004
.

Department of Defense (DoD) (November 2006). Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority. Washington, D.C..

Dessimoz, D., Jonas, R., Champod, C. & Drygajlo, A. (2006). Multimodal Biometrics for Identity Documents. Research Report. University of Lausanne: Foundation Banque Cantonale Vaudoise.

Down, M.P. & Sands, R.J. (2004). Biometrics: An Overview of the Technology, Challenges and Control Considerations. Information System Audit and Control Association, Vol 4.

English, A., Means, C., Gordon, K and Goetz, K. (2006). "Biometrics: A Technology Assessment." Ball State University. Retrieved from World Wide Web, on 20 March 2008 from http://www.bsu.edu/web/awenglish/SCHOOL/ITEDU_510/ta.html#reference.

Executive Order 9397 (3 CFR (1943-1948 Comp.) 283-284).

Föhrenbach, G. (2006). Transatlantic Homeland Security and the Challenge of Diverging Risk Perceptions. In E. Brimmer (Eds,). Transforming Homeland Security: U.S. and European Approaches (pp. 43-58). Washington, DC: Center for Transatlantic Relations, 2006.

Garfinkel, S. (2000). Database Nation: The Death of Privacy in the 21st Century. Sebastopol, California: O'Reilly and Associates.

Gugliotta, G. (1999). The Eyes Have It: Body Scans at the ATM. Washington Post. 21 June 1999. A1.

Hopkins , R. (1999) . An Introduction to Biometrics and Large Scale Civilian Identification. International review of law, computers and technology; vol. 13 (1999), No. 3, (337-363), 338.

Hon, A.R. (January-February 2008) The New Legs Race: Critical Perspectives on Biometrics in Iraq. Military Review.

International Biometric Group (IBG) (2009). Typical Iris Recognition Applications. International Biometric Group. Retreived from the World Wide Web, on 15 October 2009 from http://www.biometricgroup.com /reports/public/reports/iris0scan_applications.html.

Jain A.K., Bolle R., and Pankanti, S. (1999) "Personal Identification in Networked society", Kluwer Academic Publisher, ISBN 0-7923-8345-1, 1999.

Jain, A. K., Pankanti, S., Salil P., Hong, L., Ross, A., Wayman, J.L. (August 2004) Biometrics: A Grand Challenge. Cambridge, United Kingdom, Proceedings of International Conference on Pattern Recognition.

Joint Research Centre (DGJRC), Institute for Prospective Technological Studies (2005). Biometrics at the Frontiers: Assessing the impact on Society. European Commission.

Krishnan, K.N. (2004). Developing a Police Perspective and Exploring the Use of Biometrics and Other Emerging Technologies as an Investigative Tool in Identity Crimes. Australasian Centre for Policing Research, Report Series No. 145-1.

L-1 (2009). Omni Jail Management System (JMS) Case Study: Contra Costa County, California. Office of the Sheriff. Retrieved from World Wide Wed, 15 March 2009 from http://www.l1id.com.

National Science and Technology Council (NSTC) (August 2006). The National Biometrics Challenge. Washington DC, Executive Office of the President of the United States.

National Science and Technology Council (NSTC) (15 September 2006). Privacy & Biometrics Building a Conceptual Foundation. Washington DC, Executive Office of the President of the United States.

Nock, S.L. (1993). The Costs of Privacy: Surveillance and Reputation in America. New York: Aldine de Gruyter.

Maltoni D., Maio D., Jain A. K., & Prabhakar, S. (2003) Handbook of Fingerprint Recognition, Springer Verlag.

Mocny, R. (10 December 2007) Biometrics: Unmasking Terrorists and Criminals. Washington DC., US-VISIT Program.

O'Neal, P.H. (2005). Complexity and Counterterrorism: Thinking about Biometrics. Studies in Conflict and Terrorism. Vol. 28 pp. 547-566.

Ratha, N.K. & Govindaraju, V. (2008) Advances in Biometrics. New York: Springer.

REAL ID Program Office (9 March 2007) Notice of Proposed Rulemaking: READ ID. Washington DC, U.S. Department of Homeland Security.

Retica Systems, Inc. (2008). Retica Systems, Inc. Awarded Sole Source Contract from United States Army for Eagle-Eyes ^{TM}. Retrieved from World Wide Web, on 25 October 2009 from http://www.retica.com.

Rosen, J. (2004) Naked Crowd: Reclaiming Security and Freedom in an Anxious Age New York: Random House.

Rosenzweig, P., Kocherns, A. & Schwartz, A. (2004). Biometric Technologies: Security, Legal and Policy Implications. Legal Memorandum, Vol. 12.

Ross, A.A., Nandakumar, K., Jain, A.K. (2006) Handbook of Multibiometrics. New York: Springer.

United Nations High Commissioner for Refugees (UNHCR) (2003) UNCHR Passes 200,000 Mark in Returnee Iris Testing. UNCHR Press Release, 10 October 2003. Retrieved from World Wide Web, on 15 October 2009 from http://www.un.org.pk/unhcr/press/Oct_10_03.htm.

United States Army Biometrics Task Force (BTF) (2008). Biometrics Glossary. Software Engineering Center: CECOM Life Cycle Management Command. Release 2.0.

United States Government Accountability Office (GAO) (1999). Government and Commercial Use of the Social Security Number is Widespread. Washington D.C.: GAO/HEHS-99-28.
Vacca, J.R. (2007). Biometric Technologies and Verification Systems. Oxford: Butterworth-Heinemann.

United States Patent 291 560, 1994. Biometric Personal Identification System Based on Iris Analysis, issued to John Daugman.

Woods, K. & McLaughlin, T. (2006). Using Technology to Authenticate Individuals: A Case Study. West Virginia High Technology Consortium Foundation, Journal of Innovation, Winter/Spring 2006.

Woodward, J.D., Webb, K.W., Newton, E.M., Bradley, M. & Rubenson, D. (2001). Army Biometric Applications: Identifying and Addressing Sociocultural Concerns. Arroyo Center: RAND.