USAWC STRATEGY RESEARCH PROJECT

AN ARGUMENT FOR THE USE OF BIOMETRICS TO PREVENT TERRORIST ACCESS TO THE UNITED STATES

By

Lieutenant Colonel Ray a. Graham
United States Army

Lieutenant Colonel Michael Longarzo
Project Advisor

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
03 MAY 2004		**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
An Argument for the Use of Biometrics to Prevent Terrorist Access to the United States	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
Roy Graham	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
U.S. Army War College,Carlisle Barracks,Carlisle,PA,17013-5050	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT
See attached file.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**		**28**	

ABSTRACT

AUTHOR: Lieutenant Colonel Ray A. Graham

TITLE: An Argument for the Use of Biometrics to Prevent Terrorist Access to the United States

FORMAT: Strategy Research Project

DATE: 6 December 2003 PAGES: 22 CLASSIFICATION: Unclassified

This paper considers measures that should be taken by the United States government to implement policies for a standardized personal identification system that includes the use of chip technology and biometrics to positively identify the bearer. The paper considers and expands upon the following discussion points:

-Terrorism has changed significantly in recent years, requiring different tactics, techniques and procedures to meet this asymmetric threat.

-Terrorist groups have expanded globally, and groups operate around the world without regard to borders or national boundaries. This has made it more difficult to track and apprehend terrorists.

-There has been an increase in the practice of identity theft by terrorist organizations as a technique to infiltrate agents and operatives into the United States.

- Biometric technology offers a significantly improved method for positively identifying travelers entering the United States.

The paper recommends the following:

- -That the United States adopt a standard for a biometric identification card which is required for international travel. Include iris scanning and smart card technology to make

use of embedded chip data storage, encryption and biometrics to positively identify the bearer.

-That automation architects develop a single, shared international database of terrorist suspects, violent dissidents, and criminals, which is accessible by world-wide agencies.

TABLE OF CONTENTS

VI

AN ARGUMENT FOR THE USE OF BIOMETRICS TO PREVENT TERRORIST ACCESS TO THE UNITED STATES

For many years, the United States has been a target for terrorism. In most cases, this has been based on ideological factors involving race or religion, and countless examples can be traced back to our close political, social and economic relations with the nation of Israel. Other groups have targeted us due to our global influence as "the last superpower," while some see our globally deployed forces as occupational armies or a western campaign of global expansion, and there are others who seek the publicity and recognition to boost an otherwise unremarkable cause. There are as many motives as there are splinter groups.

HISTORY AND THE CHANGING THREAT TO U.S. PERSONNEL

In recent years, terrorism has shifted from a government-based, state sponsored campaign to one of multinational terrorist networks carrying out terrorist events

independently. State-sponsored terrorism emerged in the 1980s, most notably with the taking of the U.S. Embassy in Teheran.[1] By channeling the energy, focus and finances of a national power, Iran was able to use terrorism as a political tool. The practice has also been adopted in Palestine in attacks against Israel. More recently, Saadam Hussein threatened the U.S. with terrorist acts on U.S. soil in retaliation to the pending invasion just prior to the onset of the Gulf War. These threats posed a dangerous escalation in the use of terrorism, and the very real threat of bringing terrorism to the shores of the United States. Also, the fact that a recognized leader of a country openly threatened to use terrorism brought this tactic from the fringe extremist group to the national level. In the eyes of many Middle Eastern countries, this provided a new mindset of legitimacy for terrorism as a viable alternative through government sponsorship and funding. However, it also clearly identified who the enemy was. State sponsored terrorist states such as the Taliban in Afghanistan and Saadam Hussein in Iraq have been forcibly removed from power in response to their terrorist stance and threat to other nations. Increasing pressure has also been applied to other radical

states such as Syria and Iran to control militant and terrorist extremist groups within their countries or face political, economic or military force to compel them to do so.

With the increasing span of control and influence of large terrorist organizations in recent years, these groups now operate independent of national borders. In recent years, the world has seen increased cooperation, funding and sophistication of terrorist groups. While many have retained their differing motives and desired outcomes, they have often jelled into a loose coalition with a broad common goal. These groups often join together for a common purpose, but retain their unique denominational beliefs and doctrine. They are increasingly more willing to put these aside in to achieve the common purpose of the larger movement. The old saying that “the enemy of my enemy is my friend,” comes to mind. Largely due to the influences of Isama Bin Laden

and Al-Qaeda, terrorist and radical religious organizations throughout the world are increasingly coming together in a similar manner with the United States as a common enemy. This is illustrated in quotes from a recently captured Al-Qaeda training manual;

> We cannot resist this state of ignorance unless we unite our ranks and adhere to our religion. Without that, the establishment of religion would be a dream or illusion that is impossible to achieve. Sheik Ibn Taimia said, "The interests of all Adam's children would not be realized in the present life, nor in the next, except through assembly, cooperation, and mutual assistance in overcoming their adversities."
>
> The confrontation that we are calling for with the apostate regimes does not know Socratic debates, platonic ideals nor Aristotelian diplomacy. But it knows the dialogue of bullets, the ideals of assassination, bombing, and destruction, and the diplomacy of the cannon and machine-gun.
>
> -Al Qaeda Training Manual, Dec 2001[2]

This mutual cooperation increases the complexity associated with tracking, targeting and gathering intelligence on terrorist groups, and the members are now collaborating through increasingly capable communication and data networks from greatly dispersed locations. This allows many terrorist individuals to work remotely as members of a collective terrorist group without regard to geography, facilities, or support infrastructure. The unification of these groups poses unique challenges to our intelligence, law enforcement and anti-terrorist governmental activities. The identity of specific groups have become more difficult to identify; the increased sharing of resources, ranging from intelligence to explosives have become more difficult to trace; and the spider web of covert support often exists across national boundaries, making it more difficult to assess guilt or complicity.

SCOPE OF THE PROBLEM

While the use of technology has allowed more dispersed collaboration among terrorist groups, the physical threat to individuals or property requires the presence of terrorists or destructive material at an established target location. A common characteristic of terrorist attacks is that the perpetrator must have been physically present at some point to prepare for or carry out the attack. By introducing improved identity verification controls prior to granting foreign travelers access to the United States, we can significantly reduce the arrival of potential terrorists into the United States and allow officials to detain, apprehend or deny entry to terrorist suspects. This would be no small endeavor. Each year, more than half a trillion people enter the United States, two thirds of whom are aliens.[3] The challenge is that of sifting through billions of individual identities in order to identify a very small fraction of suspected individuals. The sheer volume of data is staggering, and impossible to manage without significant dedicated automation resources. A system that is able to produce a verifiable digital identity is key to this process. An effective system must meet three important conditions;

-Accurate. It must be able to accurately identify individuals to an extremely high degree of accuracy.

-Efficient. Speed and operating system redundancy are critical to a robust and reliable system.

-Accepted. All agencies, organizations and individuals must agree to a common architecture, set of standards, and common devices in order to implement on a large scale.

RISE IN IDENTITY THEFT AS A MEANS TO INFILTRATE

Being able to identify individual terrorist suspects is one of the most significant and concrete measures that can be taken in combating terrorism. A key component of the successful terrorist event has been the ability of the perpetrator to breach the perimeter in order to carry out the terrorist attack. While this may be a physical perimeter consisting of a fence or barrier, the same applies to national boundaries,

border checkpoints, or other access control measures designed to identify, detain or apprehend terrorist suspects. The current system of immigration controls is largely unchanged over the past century, and is based on paper documents such as passports and visas. These are intended to verify the identity of the bearer, and a photograph is the verification medium. This presents a material weakness in immigration controls. Only two components are required. The individual possesses the physical passport, and the photograph is a reasonable likeness of the bearer. In looking for ways to enter the United States or other areas undetected, terrorists have not been blind to the increase in identity theft in the United States. According to the Federal Trade Commission, more than 27 million Americans have been victims of identity theft in the past five years, with 9.9 million cases in the last year alone.[4] While most identity theft has been in the arena of economic crime, an increasing number of terrorists are turning to identity theft in order to mask their movements and to infiltrate potential target locations. Zacharias Moussaoui, a suspected terrorist in the September 11, 2001 attack on the World Trade Center, and Marwan al-Shehhi, a suspected hijacker believed to have piloted United Airlines Flight 175 into the south Trade Center's tower, are both suspected to have received money from Ramzi bin Alshibh using the stolen identity of an Arizona doctor.[5] By posing as someone else, Ramzi bin Alshibh was able to distance himself from the suspected hijacking ringleader, Mohamed Atta, who he had shared an apartment with in Hamburg, Germany in the summer of 2001. The real Arizona doctor, Ahad Sabet, had lost his passport on vacation a few years ago in Spain, when he was robbed on the street and the attackers stole his fannypack.[6] This is a clear case that demonstrated that personal information, if not properly safeguarded, is a prime source for terrorist or criminal gathering and illegal use. Also, with a minimal amount of effort, public information is available to those who readily seek it, which can lead to identity theft and other nefarious activities. This is illustrated by the previously mentioned Al Qaeda Training Manual;

> "Using public source information only and not resorting to illegal means, it is possible to gather at least 80% of information about the enemy."
>
> -Al Qaeda Training Manual, Dec 2001[7]

A benefit to using publicly available information is that the terrorist significantly reduces the risk of detection and apprehension. They are generally using legal means to gain the information, and have not committed a crime at that point. In addition to the relatively simple technique of identity theft, terrorists have also resorted to radical means to mask their identity including plastic surgery. Riduan Isamuddin, also known as Hambali, was the alleged architect of numerous attacks in the past 10 years, including last year's Bali bombing. Until his recent capture in Bangkok, Thailand, he had been masquerading in Malaysia for three months under a false identity. He had entered Thailand under a false passport, and according to a Thai police general, he had shaved his beard, trimmed his moustache and undergone plastic surgery to disguise himself.[8] As terrorists become more sophisticated in their techniques to avoid capture, the international community clearly needs a more secure means to verify a person's identity than papers and photos.

PROTECTIVE MEASURES TO INCREASE INDIVIDUAL IDENTITY AND ACCESS CONTROLS

Administration officials as well as private sector transportation organizations are growing increasingly concerned about the threat that terrorists pose. Not only do they pose a threat to the country once inside, the September 11, 2001 airplane attacks proved that they also pose a direct threat to the safety of airline personnel, passengers, and aircraft. Following the attacks in September, 2001, Pierre Jeanniot, the head of the International Air Transport Association (IATA), called for more stringent measures for airports and airlines, including the use of biometrics.[9] In order to adopt an effective system to identify potential terrorists, one single, standardized system of individual identification needs to be adopted universally for all foreigners seeking

entrance to the United States. Coupling this with an international criminal and terrorist database which is capable of data mining information concerning past travel, current itineraries, criminal background and terrorist associations, law enforcement activities would have a very powerful tool in putting a name and a face to the potential terrorist. This system must be secure, reliable and accessible, while safeguarding the privacy of the bearer.

In simple identity theft, the perpetrator steals information such as a credit card number or social security number and uses it as though they were the valid holder. By possessing this private piece of information, they are able to establish to a certain degree that they are who they claim to be. The thought process is that if they have this information, they are likely the valid holder. The same concept is used by banks and other institutions to verify over the phone a mother's maiden name, date of birth, mailing address, phone number, etc. If an idividual has access to this privileged information, they are likely to be who they say they are. A more complex identity theft is to steal source documents such as birth certificates or passports, which criminals in turn use to obtain other credentials in the valid owner's name. The credential-issuing agency may only require a single document or element of sensitive personal information that establishes the identity of the holder. By presenting false identity documentation, they are able to obtain a second generation document such as a driver's license that combines the stolen identity information with their own photograph, fingerprint or other unique identifiable characteristic. These single source verification methods only provide weak security in establishing the identity of the holder. A digital identification system, that goes beyond simple single document verification, is the best candidate to confirm individual identity through the use of unique individual characteristics, or "biometrics."

BIOMETRICS DEFINED

Biometrics are those unique, measurable characteristics or traits that each

human being possesses that can be used to automatically recognize them or verify their identity. Biometrics are seen as especially "unique" identifiers, as they are incapable of being lost, changed, or forgotten. Just as fingerprints are unique to each individual, there are many other measurable facets that can also be used, and are very difficult, if not impossible, to fake. By combining a system that can compare the biometric input to an identity database, immigration officials would have an exponentially improved method of verifying an individual's identity.

TECHNICAL ISSUES AND COMPLEX OBSTACLES TO OVERCOME

The biggest weakness that I see in establishing an automated identity verification system is the initial identity verification of an individual. If a weak identification method such as birth certificate or social security card is used, an individual will be able to establish a false identity which is entered into the system along with their biometric template, which they will be able to use repeatedly if not detected through other means. Initial identity verification may require more intrusive testing such as blood tests, DNA analysis, or other means to firmly establish identity. Once the identity is established, it remains permanently linked to the initial biometric template taken upon enrollment into the system, and becomes the fused baseline for that particular individual.

In order for a biometric identification system to be feasible, it must be fast, reliable, compact, deployable, and potentially able to share information in real time over long distances. If the system is reliant on network or communication system connectivity, and is slow or off-line, it would have devastating effects on international travel. If even one percent of all readings were false positives, millions of people would be unnecessarily detained each year. Accuracy is critical, and poses the greatest technical obstacle.

A common misconception of biometric measures is that the readings are always exactly the same. This is simply not the case. A fingerprint scanner, for

example, captures an image of the entire fingerprint as it is applied to the device, but only certain unique aspects of the fingerprint are digitally mapped for comparison. The angle and pitch that the finger is placed on the scanner, the amount of pressure applied, the moisture, body oil, skin condition, even the time of day, all cause minute factors which will vary slightly each time a reading is taken. The biometric templates vary with each biometric placement or recording: the same finger, placed over and over again, generates a slightly different pattern each time. As this data is digitized, it leads to a different string of numbers (i.e. a template). The master biometric template used to identify the individual must be able to take these variances into account while maintaining a very high accuracy level. By establishing a number of "anchor points" from a master template, a computer analysis is used to identify common characteristics and patterns to verify a match. Without a matching algorithm to make sense of a user's enrollment and verification templates, the small differences at each reading would make them appear as a mismatch, or unrelated.[10] Therefore, a verification template that takes into account these minor variations is necessary to have a high degree of probability of identity verification. The objective is to have an extremely accurate system with a very high match rate and low error rate. These parameters are defined as "False Acceptance Rates" and "False Rejection Rates."[11] The False Acceptance Rate is the rate at which the system erroneously allows an imposter to be accepted by the system. The False Rejection Rate is the rate at which a genuine user is rejected by the system. The optimum is somewhere between the two extremes where these rates cross. In other words, to achieve the best acceptance rate of valid users with the least number of false rejections. Common rates at this cross-over point for most biometric systems is in the 0.1% range.[12] These individuals would require additional scrutiny to positively verify their identity.

BIOMETRIC SYSTEMS

I will consider the advantages and disadvantages of several systems that add

the assurance of identity verification to ensure the individual is who they say they are. The steps in biometric identity verification as part of access security boil down to either identifying an individual remotely to determine who they are, or using direct individual interface reader technology to confirm or deny that they are who they claim to be. Remote methods such as facial recognition do not rely on interaction with the individual, and can be used with or without their knowledge or consent. Other methods such as fingerprint scanning rely on interaction with the individual and often some action on their part to comply. First, I'll look at those systems that seek to verify an identity claim, then look at more remote systems to identify individuals with or without their knowledge or input.

FINGERPRINT VERIFICATION.

The use of fingerprints to establish an individual's identity has been the most commonly used of all biometric measures. To incorporate this into an identity verification system, it would involve the use of an optical scanner. The subject places a specified finger or thumb on the scanner, and it scans a digital image of the fingerprint or thumbprint. Technology varies widely, but most fingerprint scanning systems create a map of the fingerprint's *minutiae*, or unique characteristics such as the distance between swirls, patterns, common points of reference or fringe patterns.[13] Some devices can detect if a live finger is present, others cannot. These systems are generally accurate if users are disciplined properly in applying the finger to the reading device. These are relatively low cost, small in size, and can be integrated into PC driven systems very easily. There are drawbacks to this method. It requires a finger to be applied to a scanner. What if the individual's finger is missing, altered, injured or otherwise changed from the original image capture? Also, it involves the compliance of the individual and the individual realization that they are being scanned. There is also a hygienic concern about the transfer of disease or infection with the large volume of individuals touching the same scanner. While there are some drawbacks, this is

currently the most common biometric method in use. Canadian customs use a system called CANPASS, which scans truckdriver's fingerprints to allow their passage across the U.S. Canadian border.[14]

HAND SCANNER

This method is similar to the fingerprint scanner, but it uses an algorithm based on hand geometry. This measures the physical characteristics of the user's hand and fingers. Methods differ in hand scanners, such as reading unique hand characteristics from a three-dimensional perspective.[15] Other scanners measure the creases on the palm, while another specializes in analyzing the veins, arteries and fatty tissues on the hand.[16] This requires less precision in hand placement on the scanner than the fingerprint scanner, and would be a good choice for untrained users such as airline passengers. This has the same potential disadvantages as the fingerprint scanner, but using a scanner that scans in three dimensions without needing the subject to touch it could alleviate the hygienic concern. The U.S. Federal Bureau of Prisons is using this biometric measure for the access control of prisoners to cafeterias, hospitals and recreational lounges.[17] The master template, first scanned when they enter the prison population, is stored in a prisoner biometric database. This database provides the comparison against the master template when a prisoner uses a hand scanner. If the hand presented to the scanner matches the master template, access is granted. Also, information about the transaction can be stored as an audit trail for prisoner tracking purposes if necessary.[18]

EYE SCAN

There are two primary methods being developed that relate to the eye, the retinal scan and the iris scan. The Retinal Scanner involves the use of a low-level infrared light source with an optical coupler that scans the eye retina.[19] It maps the image of the retina, including the pattern of blood vessels in the eye. This data is digitized, and

mapped much like the fingerprint scanner. This system is very accurate, but requires the individual to look into the scanner and focus on a given point. This process can be complicated by glasses or sunglasses, and individuals who are blind, have cataracts, are unable or unwilling to open their eye, all pose problems for this technique. The low-level infrared beam that is transmitted into the eye causes a degree of user unrest at this invasive process, and many fear eye damage as a result. This lack of public acceptance is a serious hindrance to this otherwise effective method. The retinal scan provides roughly the same volume of data and accuracy as the fingerprint scanning technique. The other optical scanning method is the Iris Scanner, which uses conventional camera technology to measure and map the iris of the eye. This technique was pioneered in England in the mid-90's, and uses the unique pattern of the colored ring surrounding the pupil of the eye (Iris). This accurate method performs better than the retinal scan on an individual wearing glasses. It is also non-invasive, in that it takes a picture of the iris rather than projecting a beam into the eye as with the retinal scan.[20] The Iris scan is considered by many experts to be the most accurate of all the biometric technologies. EyeTicket, an American company that produces iris scanners, claims that it reads 266 different characteristics (data points or anchor points) as opposed to fingerprint technology, which reads about 90. Also, the iris does not change in an individual after they are one year old, so a master template taken early in life will remain valid for a lifetime.[21] EyeTicket has run pilot programs at airports in Charlotte, NC and Frankfurt, Germany. It was also used to verify the identity of airport crews and staff in Sydney Australia during the 2000 Olympics.

DNA/BODY FLUID ANALYSIS. As anyone who has seen a recent crime drama knows, body fluids and DNA are a very good way to verify individual identity. However, due to the legal limitations on gathering samples, the lengthy testing period, complexity and cost, it is not a viable alternative for use as part of the immigration control process.

VOICE RECOGNITION.

Through the use of speech pattern analysis, voice recognition systems have generally been adopted to technology involving telephone systems.[22] These are affected by differences in communication systems, background noise, and require the individual to speak into a microphone to accomplish the analysis. The biometric template for this method is based on a master voice template, which is composed by speaking a phrase, or sentence multiple times. This is used to establish a voice template of the specific timing of speech, frequencies, timbre, and tone. This method is considered by many to be the weakest biometric method currently under study. It has trouble compensating for the differing behavior of the subject while rendering a sample, and is affected by sickness, drugs and emotions of the test subject. Also, an individual unable or unwilling to speak could not be verified using this technology.

SIGNATURE VERIFICATION

This method involves the use of scanning technology to verify an individual's signature.[23] Most systems use a stylus and input screen which require the individual to sign their name on the input screen. The scanner digitizes the signature and compares it to a signature on file. This method has more public acceptance than others in that individuals routinely sign their name, and this is a commonly accepted form of proving their identity. This is a fairly accurate medium, although not currently in widespread use.

FACE RECOGNITION.

This technique uses camera technology to scan faces. The scanned facial image is then digitized, and compared to a database that is based on facial proportions and distances between facial features.[24] By measuring the peaks and

valleys of the face, such as the very tip of the nose in relation to the depth, angle and distance to the eye sockets, nodal points are mapped and stored. Most systems use about 80 nodal points, with 14 to 22 matches needed to identity verification.[25] Advances in this technology have developed quickly, although there is a relatively high error rate. Acsys Biometric Systems, a leader in facial recognition, reports their best system has only a 3.1% error rate.[26] This seemingly small error rate would be very significant given the huge volume of daily travelers who cross our borders. Other limitations of the system include the need for ideal lighting conditions and facial angle, which have a significant impact on accuracy. Much work is being done to develop adaptive computer software that can adjust for different lighting and angles, but this method still falls far behind other techniques in accuracy. This is one of the few technologies that can be used without the subject's knowledge and can operate from a distance. For this reason, law enforcement activities and some private industries have embraced it. Over 100 gambling casinos in the United States use this technique to locate and identify known card sharks, card counters and criminals whose images are stored on a shared database.[27] Because the system measures geometric aspects of the face, it has proven to remain fairly accurate for individuals wearing a disguise or who have undergone minor plastic surgery to change their appearance.

The facial recognition system also presents a privacy concern in the minds of many individuals. By remotely scanning without an individual's knowledge, there is no specific consent given or needed to accomplish identification. The other systems involve the subject doing something, such as touching a scanner, which provides an implied consent, as they are cooperating with the process. The anonymous nature of the facial recognition system that makes it appealing to law enforcement is the same aspect that cause privacy advocates to oppose it.

SMART CARD

The “smart card” is not a biometric measure, but is used in partnership with one of the biometric systems. It is commonly understood to be a card that has the ability to store data, usually through a small computer chip embedded in the card. A smart identification card can contain personal information belonging to the bearer such as blood type, home address, etc. Given the increased storage capacity of microchips and technological advances in miniaturization and data storage, the use of a smart identity card can also be used as an identity verification device in conjunction with a biometric measure as described above. A smart card system has the capability to add additional layers of identity verification. In addition to verifying what the individual has (birth certificate, passport, credit card) and what they know (sensitive personal information, account numbers, passwords), the system can add a much stronger layer through the use of biometrics, with the personal, physical (biometric) information embedded on the card itself. The data storage mediums on the smart card vary. These may be printed data (weakest) to bar code, magnetic strip, holograph, or embedded data chip. By embedding a measurable physical characteristic (biometric) on a card in possession of the bearer (token device) a powerful link is established to verify identity. This process involves the identification of physical characteristics matched against other known information to positively identify that the person presenting a smart card is the same individual whose identity is matched to that card. As an additional layer of security, the chip on the card can contain an encryption algorithm, which encodes the biometric template. Once the encrypted card is scanned by a smart card reader, the algorithm would be matched to a decryption key, making the data readable in matching the card sample against the biometric being presented. This means that an individual’s personal biometric profile would be safe from identify theft if the card were lost or stolen. The data would be unintelligible to a thief without the key to the encryption. This application strengthens the ability of the system to protect individual privacy and secure personal information at the same time.[28]

One additional component which can be embedded in the smart card promises additional security to track both passengers and baggage. A small radio-frequency (RF) tag can be imbedded in the smart card or baggage tags, which can be read by sensors when the RF tag comes into the physical proximity of the reader. This would allow tracking of passengers and baggage within airports, as well as providing an initial identity indication when a passenger approaches a check-in point. For example, as passenger John Smith approached a smart check-in terminal, he would pass in near proximity to an RF reader, possibly imbedded in an archway or stanchion. This reader would interrogate the RF chip on his smart card. In response to the query, the reader identifies from the RF tag that the smart card belongs to John Smith. As Mr. Smith reaches the check in point, he is greeted by-name, with reservation and flight information immediately available to confirm his itinerary. He is asked to present his smart card, which is inserted into a card reader. He is then asked to submit a biometric sample (eye scan, fingerprint, etc.). Simultaneously, the biometric algorithm (which is contained on the data chip of his smart card) is applied to the decryption key, and Mr. Smith's biometric template is matched to verify that the template contained on the card matches the sample that is now being taken. In other words, the John Smith whose data is on the card is the John Smith now giving the sample at the check in point. This process would speed both initial check-in and subsequent passenger processing. Once his initial identity verification has been accomplished, John Smith would pass into a passenger-only area, and his bags, also containing RF tags, would start the loading process. By placing RF sensors or gateways at different points throughout the airport, the passenger/baggage tracking system could track the location of John Smith and his bags. Upon arrival at the boarding gate, an RF sensor could verify Mr. Smith's boarding of the plane without additional paperwork or passenger checking. It could also verify that both John Smith and his bags are on the aircraft prior to departure. A significant advantage of the smart card with biometric data is that verification can be done locally. That is, the card reading device can

decrypt the biometric and match it against the biometric sample being given without having to access a network or master database. This would be much faster than a networked system, and not subject to system down time, overload, etc.[29] This process would also have the added benefit of speeding passenger processing and requiring less physical interaction with multiple ticket agents.

DATABASES

A key component to making personal identity verification is the use of databases that contain personal information about individuals. There are fairly widespread concerns about respecting the privacy of individuals, and there are legal limitations on what information can be stored and used. The best use of database technology would be a comprehensive database, containing key information about everyone, which could be accessed or mined in an effort to detect terrorists attempting entry into the United States. This, however, is very impractical. The number of records would be astronomical, and the database impossible to assemble and maintain. Also, it would contain information about private citizens who are not suspected of wrongdoing. In 1967, Alan Westin defined privacy as "the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others." Aside from the ethical issue of maintaining detailed records about innocent citizens, laws prevent much of it. The Privacy Act of 1974 protects citizens from the unauthorized disclosure or use of their social security number, while the Computer Fraud and Abuse Act restricts cross matching of federal databases to triangulate identity information.[30] The Department of Defense was forced to do away with the Total Information Awareness Program (designed to data mine personal information for terrorist activities) because it collected information about U.S. citizens. The Department of Defense is prohibited from monitoring the private activity of U.S. citizens by privacy laws and is also barred from

operating as part of domestic law enforcement operations.[31]

Two of the major privacy concerns among opponents of biometrics are unauthorized use and unauthorized disclosure. Unauthorized use is the use of the information for a purpose other than which it was intended. Unauthorized disclosure is the widespread sharing or distribution of this personal information without consent (also possibly for uses other than the originally intended purpose of personal identification). There are opposing forces at work in the scope of information sharing. To those in the privacy extreme, this information should not be stored on any database or archive. To the other extreme, law enforcement, immigration, and anti-terrorist officials would argue that the more this information is collected and shared between governmental agencies, the better they can cooperate in the identification, detention and apprehension of potential criminals or terrorist suspects. Due to the many practical and legal limitations of a comprehensive database, the scope should be narrowed to a database of known or suspected terrorists who are not U.S. citizens. Depending upon the technology being used, part of this database may contain biometric information to assist in identity verification. This biometric information is, in fact, personal information, and should be subject to the same safeguards as other sensitive information such as hospital and financial records.[32]

CONCLUSION

To counter privacy concerns while providing the most effective personal identification system, I recommend the adoption of the Iris Recognition biometric with microchip smart card technology as the primary means of personal identification. This is the easiest, most accurate and fastest method of biometric measurement. A fingerprint biometric should be used as a backup for those limited individuals who cannot render a readable Iris scan. The biometric information should be encrypted and stored on the smart card, but not maintained on a central database. The only database checks that should be accomplished are those to check for known criminals or suspected terrorists

who are not U.S. citizens. This would provide an enhanced ability to identify nefarious individuals without running into significant legal roadblocks with U.S. citizens, and individuals not suspected of wrongdoing. This compromise would still allow scrutiny of the largest threat population. Also, the State Department should require individuals to verify their identity, record a master biometric, and be issued a smart travel card as a condition for issue of U.S. visas to foreigners. Compliance would be voluntary, but a condition for entry to the U.S. The cost of program administration and smart card production should be borne by the applicant as part of Visa application fees. The International Air Transport Association, which now represents nearly 280 airlines, has formed a working group consisting of members from airlines, airports, government agencies and commercial vendors, to further a biometric solution to passenger controls.[33] Progress is ongoing, and agreements on format and architecture between governmental organizations are being worked out. Hopefully, this recommendation will become a reality within the next four to six years. It is true that we sacrifice a degree of privacy and anonymity to preserve the liberty of our nation and protect its citizens from those who would do us harm. This is a small price to pay in order to secure increased security, improved immigration controls and a safer traveling environment for all.

WORD COUNT: 6005

END NOTES

[1] David Tucker, *Skirmishes at the Edge of the Empire: The United States and International Terrorism* (Westport, CT: Praeger, 1997), 2.

[2] AlQaeda Training Manual, *Declaration of Jihad*, seized by the Manchester Metropolitan Police in an Al Qaeda member's home, December 2001. Translated as evidence for the U.S. Embassy bombing trial in 2001.

[3] Paul R. Pillar, "Terrorism Goes Global, Extremist Groups Extend Their Reach Worldwide," *Brookings Review*, (Fall 2001, Vol. 19, Number 4), Brookings Institute, 34-37.

[4] "High Price of Identity Theft," *CBSNEWS.com*, September 2003 [journal on-line]; available from <www.cbsnews.com/stories/2003/06/30/national/main561084.shtml>, internet, accessed 4 September 2003.

[5] "Motion: 9/11 Conspiracy Suspect May Have Used ID of Arizona Doctor," *CNN.com/LawCenter* [journal on-line] available from <http://cnn.com/2002/LAW/08/07/inv.moussaoui.stolen.id/>; internet, accessed 5 August 2003.

[6] Ibid.

[7] AlQaeda.

[8] "Bali Bombing Suspect Had Plastic Surgery," Guardian Unlimited, available from <http://www.guardian.co.uk/indonesia/Story/0%2C2763%2C1019952%2C00.html> internet, accessed 18 August 2003.

[9] "Biometrics: The Future of Security," *CBCNews*, available from <www.cbc.ca/news/indepth/background/wtc_biometrics.html>, internet, accessed Oct 17, 2003.

[10] "IBG Bioprivacy Initiative," *IBG Group*, available from <http://www.bioprivacy.org/> internet, accessed 14 August 2003.

[11] Julian Ashbourn, "Biometric White Paper," 1999, available from <http://homepage.ntlworld.com/avanti/whitepaper.htm>, internet, accessed 15 August 2003.

[12] Ibid.

[13] Ibid.

[14] Biometrics.

[15] Ashbourn.

[16] Biometrics.

[17] Ibid.

[18] Ibid.

[19] Ashbourn.

[20] Biometrics.

[21] Ibid.

[22] Ashbourn.

[23] Ibid.

[24] Ibid.

[25]Biometrics.

[26] Acsys Biometrics Corporation, available from <http://www.acsysbiometrics.com/product.html>; internet, accessed 14 August 2003.

[27] Biometrics.

[28] "Privacy and Secure Identification Systems: The Role of Smart Cards as a Privacy Enabling Technology," *Smart Card Alliance*, February 2003, internet, available from <www.smartcardalliance.org>, accessed Oct 17, 2003, 3.

[29] Biometric White Paper.

[30] "Identity Management," The National Electronic Commerce Coordinating Council, presented at the NECCC Annual Conference (December 4-6, 2002, New York, NY), available from www.ec3.org, internet, accessed 26 October 2003.

[31]William Matthews, "DOD Set to Use Data Mining in the Global War on Terror," *Army Times*, December 8, 2003, p. 23.

[32] IBG.

[33] 3M Security Market Center Industry Links, available from <http://www.ait.ca/html/partners.html>, internet, accessed 26 October 2003.

BIBLIOGRAPHY

3M Security Market Center Industry Links, available from <http://www.ait.ca/html/partners.html>, internet, accessed 26 October 2003.

Acsys Biometrics Corporation, available from <http://www.acsysbiometrics.com/product.html>; internet, accessed 14 August 2003.

Ashbourn, Julian "Biometric White Paper," 1999, available from <http://homepage.ntlworld.com/avanti/whitepaper.htm>, internet, accessed 15 August 2003.

Author Unknown. AlQaeda Training Manual, *Declaration of Jihad*, seized by the Manchester Metropolitan Police in an Al Qaeda member's home, December 2001. Translated as evidence for the U.S. Embassy bombing trial in 2001.

"Bali Bombing Suspect Had Plastic Surgery," Guardian Unlimited, available from <http://www.guardian.co.uk/indonesia/Story/0%2C2763%2C1019952%2C00.html> internet, accessed 18 August 2003.

"Biometrics: The Future of Security," *CBCNews*, available from <www.cbc.ca/news/indepth/background/wtc_biometrics.html>, internet, accessed Oct 17, 2003.

"High Price of Identity Theft," *CBSNEWS.com*, September 2003 [journal on-line]; available from <www.cbsnews.com/stories/2003/06/30/national/main561084.shtml>, internet, accessed 4 September 2003.

"IBG Bioprivacy Initiative," *IBG Group*, available from <http://www.bioprivacy.org/> internet, accessed 14 August 2003.

"Identity Management," The National Electronic Commerce Coordinating Council, presented at the NECCC Annual Conference (December 4-6, 2002, New York, NY), available from www.ec3.org, internet, accessed 26 October 2003.

Matthews, William "DOD Set to Use Data Mining in the Global War on Terror," *Army Times*, December 8, 2003.

"Motion: 9/11 Conspiracy Suspect May Have Used ID of Arizona Doctor," *CNN.com/LawCenter* [journal on-line] available from <http://cnn.com/2002/LAW/08/07/inv.moussaoui.stolen.id/>; internet, accessed 5 August 2003.

Pillar, Paul R. "Terrorism Goes Global, Extremist Groups Extend Their Reach Worldwide," *Brookings Review*, (Fall 2001, Vol. 19, Number 4), Brookings Institute, 34-37.

"Privacy and Secure Identification Systems: The Role of Smart Cards as a Privacy Enabling Technology," *Smart Card Alliance*, February 2003, internet, available from <www.smartcardalliance.org>, accessed Oct 17, 2003, 3.

Tucker, David. *Skirmishes at the Edge of the Empire: The United States and International Terrorism*. Westport, CT: Praeger, 1997.