NATIONAL DEFENSE UNIVERSITY

NATIONAL WAR COLLEGE

TRANSFORMING SECURITY SCREENING WITH BIOMETRICS

Lt Col BRIAN J. HEARNSBERGER, USMC
CORE COURSE 5605
DOING NATIONAL MILITARY STRATEGY

EXPANDED AND SEQUENTIAL PAPER

FACULTY SPONSOR
MR. THEODORE LAVEN

ADVISOR
COL. GARY L. WILLISON

9 APRIL 2003

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
09 APR 2003		**09-04-2003 to 09-04-2003**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Transforming Security Screening with Biometrics	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **National War College,300 5th Avenue,Fort Lesley J. McNair,Washington,DC,20319-6000**	8. PERFORMING ORGANIZATION REPORT NUMBER
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
The original document contains color images.

14. ABSTRACT
see report

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**		**26**	

TRANSFORMING SECURITY SCREENING WITH BIOMETRICS

How would you feel about having your face scanned and compared against your military identification card when entering a base? How about submitting your fingerprint before entering an airport security area and boarding a plane? Facial scans and fingerprinting are just two examples of biometrics, "the automated use of physiological or behavioral characteristics to determine or verify identity," that can reduce fraud and identity theft to dramatically improve physical security.[1] Today, biometric technology could be implemented to transform physical security by enhancing screening procedures currently in use at U.S. bases worldwide and government-operated screening points throughout America.

Background

The Department of Defense (DoD) has been experimenting with biometric identification for over 10 years and even established a Biometrics Management Office a few years ago to oversee the development and implementation of biometric technology in the Armed Services.[2] Most DoD research has been aimed at logical access solutions such as the protection of automated information systems and other computer-based applications. Tragedy brought about renewed interest in innovative solutions to a major physical security problem: screening individuals.

A 1996 terrorist attack on Khobar Towers, a building in Saudi Arabia that housed U.S. Air Force personnel, prompted the Defense Advanced Research Projects Agency to experiment with facial recognition technology for identification of known terrorists. While DoD has been accelerating biometrics research ever since, the Department has yet to implement any technical means to supplement the screening of personnel accessing military installations and services. Fingerprint readers, hand geometry machines, voice recognition devices, iris scanners, and other

authentication devices are only randomly used for high security areas such as planning and operations centers, but are not employed for general access to military bases.

The Al Qaeda offensive on 11 September 2001 demonstrated just how vulnerable the United States is to the threat of global terrorists. Their attacks on the World Trade Center and Pentagon revealed weaknesses in physical security screening and prompted renewed congressional interest in domestic security. Congress held hearings and listened to countless witnesses address biometric solutions to counter the threat of terrorists since 9/11.

Requiring a fingerprint or other biometric sample to be provided in order to obtain a form of identification offers a unique method to identify individuals that would be particularly useful for tracking and apprehending known or suspected terrorists and other lawless elements of society. However, using biometric technology as a verification or identification tool for physical security screening in the public domain raises new questions about individual privacy rights. Senators and congressmen proposed legislation to standardize state driver's licenses and identification (ID) cards that would have included biometric identifiers, but Congress has been unable to enact any relevant legislation. Congressional concern about safeguarding U.S. citizens from the global threat of terrorism wanes as time dampens recollections of the 9/11 attacks. Alternately, congressional concerns for individual privacy rights heighten as memories of the 9/11 attacks dim.

Facing increasing global terrorism threats, the United States has tightened physical security and increased the frequency of screening, but has yet to leverage biometric technology to enhance security screening. Army National Guardsmen have been activated to enhance the physical security of Air Force bases around the world due to the shortage of Air Force security personnel during the global war on terrorism. Commercial airport terminal security personnel

have been increased threefold to scrutinize the screening of travelers. Security personnel throughout America, including DoD, go through the motions every day taking cursory looks at ID cards and randomly checking possessions and vehicles for weapons and explosives. The U.S. is expending immense fiscal resources and human capital to increase security-screening efforts, but has yet to take advantage of biometric technology in the year and a half since 9/11.

Our technical complacency increases the likelihood that America will have to absorb more terrorist' blows in the fight against radical, extremist organizations. To improve national security and homeland defense, America must begin using technology to supplement, and sometimes replace, archaic human-based screening procedures today. Right now, biometrics can be the transformation technology of the physical security realm.

So why hasn't the U.S. Government leveraged biometric identification and verification technology to improve personnel security screening methods? This paper exposes the challenges of enacting national legislation that would require the collection of a biometric sample before states could issue driver's licenses and other forms of identification. It also takes a look inside DoD and proposes that the Department transform military physical security screening procedures by using existing biometric technology as the first line of defense against terrorists and other lawless elements that cause havoc through fraud and identity theft.

Congressional Interest in Biometric Security

Members in the U.S. House of Representatives and U.S. Senate introduced legislation during 2002 aimed at improving state-issued licenses and other ID systems to reduce fraud and identity theft by including biometric identifiers for physical security screening. Two bills were proposed; both stalled in committees and later died when the 107th Congress concluded business last fall. The following paragraphs describe the politics surrounding national legislation to enhance the

integrity of state driver licensing systems and predict actions the 108th Congress will take to enhance identity security through standardization.

Most Americans would agree that we need licenses and IDs that are more secure and less likely to be forged or easily manipulated to steal another's identity. It seems unlikely that legislation designed to improve physical security screening, reduce fraud and limit identity theft would be controversial. However, after reviewing the history of House and Senate proposals and talking with congressional staffers, it became evident that legislation to reform license and ID procedures has been, and will continue to be, a much-disputed topic.

At the heart of the controversy is the management and control of personal information. This includes biometric data, "a nationwide unique identifier," such as a fingerprint or iris scan that would be provided to state authorities before an individual receives a license or ID.[3] The language in two legislative bills about "linking state motor vehicle databases" appears to be a national identification system.[4] However, Americans have consistently rejected the idea of national ID cards as an invasion of privacy for fear of unreasonable searches and seizures.

Recent Legislation

Driver's License Modernization Act of 2002 (H.R. 4633). Congressman James Moran (D-Va. 8th) introduced House Resolution 4633 on 1 May 2002 with the support of Tom Davis (R-Va. 11th). The House bill calls for states to have a license and ID system that: (1) uses computer chips on cards to hold personal data including biometrics, (2) obtains and maintains biometric data on individuals, and (3) is linked electronically to state motor vehicle databases.[5] This bill was referred to the House Subcommittee on Environment, Technology and Standards on 23 May and set idle for the remainder of the 107th Congress amid controversy that the proposed legislation advocates creating a national identification system.

Driver's License Fraud Prevention Act (S. 3107). Senator Richard Durbin (D-Il.) introduced Senate Resolution 3107 on 10 October 2002 with the support of John McCain (R-Az.). The Senate bill calls for: (1) a study to determine if there is a need for a "nationwide unique identifier system [biometric data]", (2) development of an agreement to facilitate sharing of driver's license and ID records among states, and (3) consolidation of national license and ID information systems into a new Driver Record Information Verification System (DRIVerS).[6] The bill was referred to the Senate Committee on Commerce, Science and Transportation the day it was introduced and died with the conclusion of the 107th Congress. While S. 3107 can also readily be interpreted as a step toward a national identification system, it places most of the burden for determining the criteria for license standardization on the Secretary of Transportation.

A central point of controversy surrounding these bills is the management of personal data that individuals provide to state authorities before receiving a license or ID. Both legislative bills mandate the collection of biometric information such as a fingerprint or iris scan from individuals and vaguely describe a national database of unique identifiers. To most people, maintaining information in a national database that could be used to determine or verify a person's identity sounds like a government science project or movie with the purpose of conducting surveillance on U.S. citizens.

To civil libertarians, these bills look like attempts to establish a national ID card system and a threat to the 4th Amendment privacy rights afforded to U.S. citizens. Privacy risks and identity security are the main concerns that opposition groups have brought to the attention of Congress.[7] To many people, license and ID standardization is nothing but "a legislated national ID card."[8] Neither bill addresses privacy concerns and both appear open-ended even though Senators and

Congressmen on both sides of the argument realize that standardized IDs with biometric identifiers would improve physical security screening.

Special Interest Power and Influence

Based on interviews with staff representatives for two senators and three congressmen, as well as testimonials during the 2002 Congressional committee hearings, it appears that lobbying efforts for license and ID standardization are paying off for their suitors. There are two distinct political action groups at work, one with House backing and one with Senate backing. Both groups speak on behalf of other special interest organizations and rally support for their self-professed cause: preventing identity theft. Each political action group found an advocate to advance their special interests and could be the reason there are parallel efforts in the House of Representatives and Senate.

The Progressive Policy Institute shepherds the interests of the Virginia biometric industry and found backing for their license standardization proposal in the House of Representatives. Congressman James Moran (D-Va. 8th) advocates their proposal to modernize state-issued licenses and IDs using unique identifiers to authenticate the oneness of cardholders. "There is heavy Virginia interest in the biometric industry."[9] The Progressive Policy Institute promotes technical solutions to legislative issues and brought forward model legislation on behalf of Virginia biometric security firms to Moran and Tom Davis (R-Va. 11th) in the aftermath of 9/11.

The Driver's License Modernization Act was developed from a research paper provided by the Progressive Policy Institute.[10] Language in the House bill mirrors that of the institute's paper.[11] When it was introduced last May, the House bill was academically orientated, heavy on biometric language and became a magnet for unfavorable commentary. Critics immediately

labeled the proposed bill as a call for a national ID card, stalling movement of the legislation and curbing the institute's efforts.

House staffers readily admitted that special interests groups drive the agenda of the Virginia congressmen they work for.[12] They appeared proud that state industry has a voice in Congress through elected representatives. "The Virginia biometric industry brought the Driver's License Modernization Act to the attention of their congressmen. Industry paved the way for this legislation."[13] House staffers left the impression that congressmen openly enjoyed their connection with local industry. On the other hand, Senate staffers left the opposite impression.

Since the mid-1990s, improving the integrity of licensing and other ID systems has been on the political agenda of law enforcement and state motor vehicle licensing agencies in the United States and Canada. Their most avid political action group for license and ID reform is the American Association of Motor Vehicle Administrators (AAMVA). The Association has been "working the hill" for years to promote legislation aimed at improving the integrity of licensing and ID systems nationwide through standardization and information sharing.[14] The events of 9/11 provided a platform for the AAMVA to renew their efforts to standardize licensing and ID systems.

With a longstanding interest in reducing identity theft, Senator Durbin (D-Il.) became an attractive advocate for AAMVA driver's license standardization proposals during Fall 2001 when concerns for improving physical security screening were at the forefront of congressional business. A victim of identity theft himself, Durbin is probably the most-influenced member of Congress with ties to the AAMVA.[15] As the Chairman of the Senate Subcommittee on Oversight of Government Management, Restructuring and the District of Columbia, Durbin

scheduled and conducted hearings during April 2002 regarding license integrity with testimony from an AAMVA representative with the aim of improving security screening.

Senate staffers denied that the AAMVA is responsible for the legislation introduced by Senator Durbin to curb driver's license fraud and identity theft.[16] After further discussion, one staffer stated "the AAMVA and the Senator came up with the idea of a Driver's License Fraud Prevention Act at the same time."[17] This is an interesting comment given that the AAMVA has a web site that includes model legislation and had a history of promoting license standardization and consolidation of driver databases long before the Al Qaeda attacks on the United States.

Clearly, the evidence illustrates that Senator Durbin is acting on behalf of the AAMVA regarding the Driver's License Fraud Prevention Act (S. 3107) that he introduced. The Association published their idea of a national standard for licenses and IDs during January 2001.[18] It wasn't until after 9/11 that Senate committees initiated hearings related to identification security and solicited testimony from ID security advocates, including the AAMVA. The Senate began discussing the concept of a bill to standardize licenses to improve security screening during October 2001.

It is interesting that House staffers openly acknowledged backing from, and advocacy for, a special interest group while Senate staffers attempted to conceal the connection that some senators have with a group promoting a driver's license standardization bill. One explanation may be that the Senate approach to standardization is probably kept low-key to avoid negative publicity. The House proposal attracted a lot of negative press during Spring 2002 and then was stalled for over six months in the same committee. Appearing to learn from the frustrations experienced in the House of Representatives, the Senate quietly introduced a license and ID

standardization bill that is less specific and void of technical language. So far, there has been only marginal criticism of the Senate bill.

Resistance and Opposition

Central to opposition groups are privacy concerns related to the Bill of Rights. The more vocal constituents against driver's license and ID standardization that includes biometric identifiers are well known to members of Congress. Civil libertarians voice opposition to standardization efforts mainly through the Electronic Privacy Information Center (EPIC). The Center has sounded the alarm, pointing out potential problems with national government proposals to standardize state-issued licenses and ID cards.[19] EPIC opposes all standardization efforts, particularly the collection of biometric identifiers and describes them as a threat to civil liberties.

To EPIC, standardization will result in greater sharing of personal information between state and federal officials. "We've lost the battle with EPIC, but not the war. They portrayed driver's license standardization as mission creep toward a national ID card."[20] EPIC has the attention of constituents by igniting fears of government monitoring to track the movement of individuals and surveillance of a person's electronic transactions. EPIC also points out that there are no limits to define the degree of information sharing allowed by license standardization and that there are lingering questions regarding the storage of personal information and its vulnerability to theft or abuse.[21]

Congressional staffers were all very familiar with the concerns of the opposition. House staffers were quick to describe how EPIC rallied support from special interest groups last summer to stall their proposal. "The calls went out from EPIC. Right wing talk show hosts slammed the proposal as an infringement of our 4th Amendment rights."[22] Staffers in both the

House and Senate shared their opinion that the constituents against driver's license standardization were mostly those with driving problems and persons concerned that the government might discover their true identity. "Millions of drivers use someone else's ID. At the top of the list are illegal aliens, deadbeat dads and DWI cases. These folks are paranoid that they will be discovered if we standardize IDs and include biometric identifiers to improve security screening."[23] Staffers left the impression that there was always room for compromise to thwart opposition concerns. Not surprising, two House staffers mentioned that they believed the Driver's License Modernization Act would be "scaled back" by removing biometric, unique identifier, language.[24] This would seriously reduce the ability of the act to reduce fraud and identity theft. All staffers interviewed stated that preserving our 4th Amendment privacy rights was a priority for congressional members and increasingly more important than improving security screening.

Balancing Security and Privacy Rights

Can we trust the U.S. Government to operate a national database of personal information on every person with a state driver's license or ID card without giving up our individual privacy? Absolutely not! We would be hard-pressed to name a government database that has not been misused by the people entrusted with the information. "The Senate intends to structure-in adequate oversight to address the concerns of civil libertarians."[25] To answer "yes" to the question posed above, Americans would have to be convinced that Congress has built-in strict controls to a license standardization bill that protects privacy and prevents misuse. The solution to this dilemma is to limit access to biometric and other personal information that states collect from drivers while including substantial oversight provisions.

The Senate bill describes a system that may answer privacy concerns but does not explain system capabilities. The Driver's License Fraud Prevention Act calls for use of the Driver Record Information Verification System (DRIVerS).[26] This system actually does restrict user access, enabling states to operate databases according to specific legislative or legal requirements through "pointer" technology.

A driver's license pointer system would allow state and federal law enforcement officials to query a national database and search for a person's name, license number, ID number, or Social Security number without having first-hand access to unique identifying information such as a photo, fingerprint or iris scan. If a name or number match occurred during a query, the system would point the using official to the state of record.[27] To obtain additional information, the official would then have to contact the state of record and meet state-specific legal requirements, such as a warrant, before having access to personal information that might jeopardize an individual's privacy. In short, officials would be required to show probable cause and legal authority before obtaining state-held personal information, including biometric identifiers and driving records, for individuals with a state license or ID. Pointer systems with proper oversight appear capable of satisfying privacy concerns.

Will the 108th Congress Pass an ID Bill That Requires Biometric Identifiers?

Privacy rights will remain at the forefront of the issue, but expect members of the 108th Congress to reintroduce bills in both the House and the Senate that would standardize driver licenses and identification cards. To enhance their chances of approval, the House and Senate will probably include language in license standardization bills that refer to "identity security" described in the Homeland Security Act adopted last November.[28] "We have to be right millions of times a day, every day, forever," said Tom Ridge, U.S. Homeland Security Director. "They

[the terrorists] have to be right once in a while."[29] Terrorist fraud and identity theft focused Congress on improving license and ID security after 9/11 and remains the principle reason for the House and Senate to continue to debate license and ID standardization legislation that includes biometric identifiers.

Congressman Moran (D-Va. 8th) will need to tone down technical language in the House resolution to assuage civil libertarians unless, of course, another catastrophic terrorist attack on America numbs Congress' inclination to assert privacy rights before national security. However, if Moran removes the requirement for states to collect and maintain a unique identifier record, the House bill will be toothless. Without the requirement for a biometric identifier, any bill would not fulfill its purpose of reducing identity theft and fraud. Moran's bill will have to address the issue of securing biometric data maintained at the state and federal level for any chance of success. Based on the strong public opposition to the House Driver's License Modernization Act he introduced last spring, and the Senate's displeasure that a House bill was introduced while a Senate version was in the works, Congressman Moran will probably not be successful in getting his bill passed.

Today, the Senate license standardization bill appears to be the one most likely to be enacted. The Driver's License Fraud Prevention Act is void of technical language and has attracted little attention from civil libertarians. Senator Durbin (D-Il.) convinced Senator McCain (R-Az.), the Chairman of the Senate Committee on Commerce, Science and Technology for the 108th Congress, to co-sponsor his bill immediately after the Fall 2002 elections.[30] If Senator Durbin revises the Driver's License Fraud Prevention Act to include language to clearly indicate that the Driver Record Information Verification System (DRIVerS) pointer system can be used to protect

our 4th Amendment privacy rights while reducing fraud and identity theft and spells out congressional oversight provisions, it is possible that his bill could be approved.

Based on the politics surrounding driver's license and ID standardization that envisions individuals providing a unique identifier, such as a fingerprint or iris scan, before a state issues a form of identification, Americans are not likely to see biometrics implemented in the public domain in the near future. On the contrary, DoD is an attractive candidate for initiating broad biometric security measures while Congress debates legislation that would affect the general population.

Today's Military Physical Security Screening Methods are Superficial and Ineffective

All Americans have been subjected to increased security measures since 9/11. Without biometric identification to supplement security guards, most screening is superficial, broad-brushed and random. In particular, DoD personnel resign themselves to countless ID checks and random vehicle inspections when entering military facilities.

Gate guards are charged with ensuring that only personnel who have authority to enter an installation are granted access. "While humans are adept at recognizing facial features, we also have prejudices and misconceptions."[31] Gate guards look at thousands of ID Cards everyday so they can't possibly ensure that every person entering an installation is not a terrorist or other suspect person that should be denied access to military facilities.

We've all seen feeble attempts by security guards using mirrors to randomly check the underside of vehicles. They merely glance at a reflective device before approving passage of each and every vehicle being checked. Overwhelmed by surging inspection requirements since 9/11, military security guards sacrifice accountability as they rush to process endless lines of vehicles randomly selected for screening. Without the aid of biometric technology to screen

individuals entering federal installations, guards are forced to randomly select vehicles or result to discriminatory methods such as profiling when making a determination of what vehicles to inspect. The same is true for Transportation Security Administration guards screening seemingly unlimited waves of airline passengers and baggage. Using biometrics to verify the identity of individuals provides an element of reliability and is an innovative tool that can enable security screeners to focus ID inspection and vehicle search efforts.

Transforming Military Physical Security Screening Using Biometrics

The DoD Biometrics Management Office created in 2000 to oversee biometric initiatives has tended to focus development efforts on logical access issues to enhance information assurance programs within the government and information technology business sector. We have yet to see any broad initiatives to utilize biometric identifiers for physical access security screening. The Biometrics Management Office has fostered experiments with Common Access Cards (CAC) that incorporate biometric identifiers.[32] A CAC is a form of ID card with an embedded microchip. Either CAC or standard ID cards are issued to DoD members. They are not required to have both cards. Common Access Card technology demonstration criteria have drifted toward logical access and information assurance, yet the weakest link in military security is the actual screening of individuals. Facial recognition technology has been tested to some degree for accessing highly sensitive military areas, but not for screening those requesting access to military installations.

The Department of Defense should implement biometric technology for physical security screening as the first line of defense against terrorists and criminal threats to U.S. military installations. There is no better way of verifying the identity of personnel entering a military facility. While Congress weighs privacy concerns involving the inclusion of biometric

identifiers on driver's licenses and other state issued forms of identification, DoD could strengthen physical security screening procedures by storing biometric samples on IDs and CACs. DoD could also use facial scanners to screen personnel entering bases and stations.

It is recommended that the DoD Biometric Management Office focus on using unique identifiers as a tool to conduct physical access screening instead of the current focus of logical access screening. The greatest threat to military security is physical access to installations, not logical access to information systems. Besides vigilance, biometric technology is the most promising means to enhance physical security in the name of homeland defense.

Integrating biometrics into physical security screening would extend the ID registration and background investigation process a person goes through before a card is issued to gate security at bases and stations. DoD members go through an extensive screening process to verify their identity before ID or CAC cards are issued. Birth certificates are submitted as proof of age, fingerprints are taken, local background checks are completed, etc. If fingerprint samples were included on ID and CAC cards when they are issued and gate guards are provided with the capability to compare the fingerprints of people requesting access to military bases with the recorded sample on individual cards then verification of a person's identity would be associated with background checks performed before issuance.

Biometrics would be extremely useful when force protection conditions are more defensive and additional gate security measures are implemented. When military bases strengthen force protection measures, guards conduct cursory inspections of all vehicles regardless of the reliability of the person being screened for entry. Because of the volume of drivers and vehicles attempting to enter military bases, guards simply do not have time for thorough searches. With biometrics to enable gate guards to assist them to determine the reliability of individuals

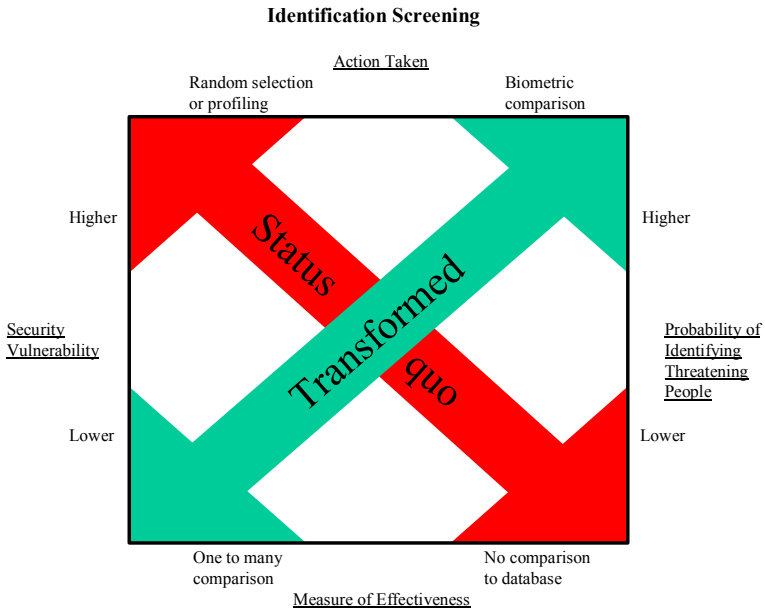
requesting base access, they would need to inspect far less vehicles during heightened force protection conditions. The fewer vehicles inspected, the more thorough search measures can be.

Using dogs and technical methods to search vehicles for hidden explosives is almost unheard of today. Yet in the post 9/11 world, the principle reason that guards at military bases are conducting vehicle inspections is to deter terrorists from using explosives. Using biometrics as a personnel reliability indicator would sharply cut the number of vehicles targeted for detailed inspection. Gate guards would have more time to use explosive detection devices to check the vehicles of "less than reliable" individuals. Transforming physical security at military gates by exploiting biometric screening would enable gate guards to focus their efforts and enhance the effectiveness of vehicle searches.

Biometrics to Identify

Even though terrorism can never be completely eliminated, DoD can take prudent steps to deter future attacks by using biometrics to scan individuals requesting base access and comparing their facial features to those of known and suspected terrorists and other lawless elements. Scanners could be used at military base access points to employ facial recognition technology for comparing individuals with a database of undesirables that constitute potential threats to base or station security.

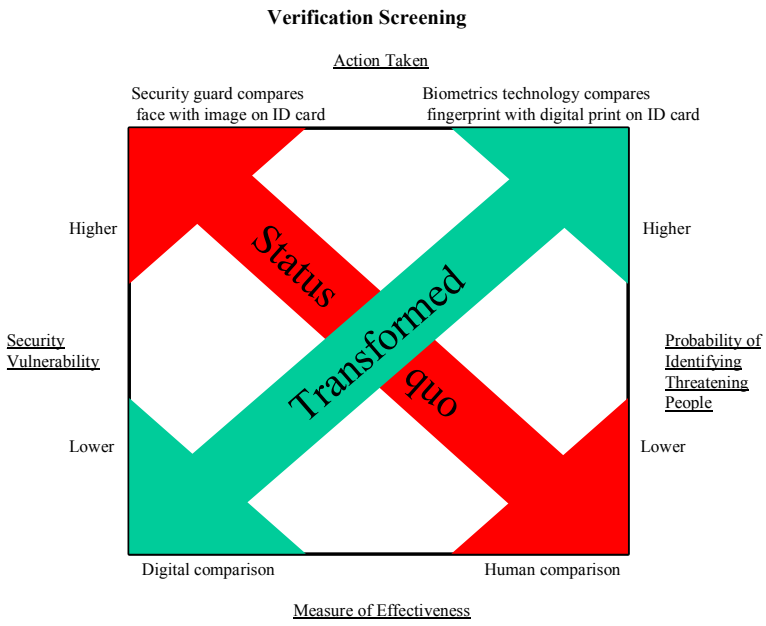
The process of identification attempts to answer the question, "Who am I?[33] Identification does not require an individual to actually claim who he or she is. A person's biometric features can be compared against database records of suspect individuals, referred to as one to many authentication. Facial scanning would be particularly useful for initial screening of all individuals accessing a military base, regardless of whether or not they possess a valid ID or CAC card to verify their identity.



While face recognition is considered an invasion of privacy by civil libertarians, the Supreme Court of the United States has found that "a person does not have a reasonable expectation to privacy in those physical characteristics that are constantly exposed to the public."[34] According to the Court, scanning of individuals in a public area does not constitute a search. Facial scanners could be utilized today as the first line of defense against terrorists.

Biometrics to Verify

Identification and Common Access Cards in use today are capable of storing an individual's biometric information within bar codes, digitized and magnetic strips, and embedded microchips in order to verify the identity of military personnel requesting access to an installation. The process of verification attempts to answer the question, "Am I who I claim to be?"[35] ID and CAC Cards can be used to store a person's biometric data for comparison with a biometric sample provided when he or she requests access. Comparing a biometric sample with information stored on a card would allow gate guards to verify that a person is who he claims to be, one-to-one authentication.[36]



By verifying the identity of personnel using biometrics, gate guards could shift their detailed inspection efforts from random vehicle selections to cars and trucks driven by those more likely to be a threat to installation security. Individuals that attempt to disguise their identity with false or stolen identification cards are the greatest threat to base security. The shear volume of personnel and vehicles to be physically checked make biometric security screening a prudent means to quickly verify that each person is who he claims to be. Biometrics provides a method to "neck-down" physical security screening to those with unreliable identity documentation.

Compulsory Biometric Security Screening

DoD already maintains fingerprints on every individual entered into service so biometric verification security could easily be implemented into military screening today. Providing a fingerprint is a condition for obtaining an ID card. The Army uses fingerprints as a biometric identifier to control the issue of Common Access Cards now. There is no reasonable expectation to privacy if a person desires to access military facilities. Military ID and CAC cards are, for all practical purposes, national identification cards since it is mandatory to have one or the other to access U.S. military facilities and services.

While DoD maintains biometric samples on individuals in centralized databases, the Department has yet to include a unique identifier, such as a fingerprint, on ID and CAC cards. The problem is not technology in this case, but the will and funding to utilize biometric screening for physical security at DoD installations throughout the world. In effect, DoD has a compulsory biometric security system already in place since a sample is collected from DoD members and dependants before an ID or CAC card is issued. But this compulsory system will continue to be "nonfunctional" unless biometrics is used during physical security screening at points of access to federal installations. Implementing biometrics as a screening tool at military bases would allow gate guards more time to concentrate on undocumented visitors.

Voluntary Biometric Security Screening

Just like airport security with its long lines and obligatory searches, accessing a military base becomes frustrating the more a person is questioned or their vehicle is inspected. Since delivery personnel and other non-DoD members requesting temporary base access do not have government issued IDs capable of holding biometric identifying information, they are not subjected to compulsory sample collection. Consequently, without unique identifier credentials they would be subjected to more intrusive physical inspections at base access points if and when biometric physical security is implemented. Like airline trusted/registered passenger programs in the works, a "registered visitor program" would be a means for non-DoD individuals to submit a biometric sample and other personal information to expedite security processing when requesting more than occasional access to military bases.

When Transportation Security Administration officials unveiled the latest version of a Computer Assisted Passenger Profiling System (CAPPS II) for use as a security screening program, the Senate Commerce Committee stalled implementation of the surveillance system for

fear that this profiling system could be an invasion of privacy.[37] While the CAPPS approach to passenger screening is consistent with generally accepted standards of nondiscriminatory profiling, it is unlikely to be implemented unless the TSA can satisfy Congressional privacy concerns. In the meantime, passengers will flock to registered traveler programs as they become available. The same is true for persons frequenting military bases without DoD credentials; they will seek means to shorten the time it takes for physical security screening.

Assuming biometric security is implemented at military base access points, failure to have a means of authentication that includes a biometric sample for verifying a person's identity would not necessarily result in denial of entry. However, individuals and their vehicles would be subjected to greater scrutiny by gate guards. Contractors and others requiring frequent but temporary access to military bases would gladly embrace a registered visitor program since it would mean less delays and streamlined physical security screening.

Benefits of Biometric Authentication During Combat

Any situation where a person's identity needs to be authenticated is a potential area for biometric technology, particularly combat. Physical and logical access control will always top the list of DoD uses during peacetime, but combat uses could benefit a fighting force. Biometric identification could assist medical personnel to access personal information such as blood type, allergies to medications, etc. for injured personnel to reduce diagnosis time and the chances of administering drugs that could result in a fatal reaction. Unique information, such as fingerprints, can expedite identification of a deceased person's remains. Biometrics could be used to protect weapons systems from enemy use, to register prisoners of war, to investigate war crimes and hundreds of other uses.

What We Can Expect

For the foreseeable future, America will be concerned about strengthening physical security due to the attacks of 9/11. There are multiple scenarios for using biometrics to improve security, but American expectations for privacy will continue to limit the use of unique identifiers in the public domain. Transportation personnel reliability programs will be so focused on employees that the effectiveness of passenger security checks will remain limited by random screening and profiling methods in use today. Unless incentives outweigh privacy fears, biometrics will not be embraced as verification or identification tools to increase military and civilian security.

Though the military can implement facial recognition to screen personnel requesting access to bases and stations, DoD is not likely to use biometrics to scan individuals unless the U.S. is subjected to sustained attacks from terrorists. Unfortunately, definitive identification will remain unimportant unless Congress and the American people can be convinced that national security is more important than privacy concerns in the public domain. Only more terrorist attacks will turn our attention from individual rights to more effective screening methods in the interest of national security.

Automobile insurance companies may one day offer motorists incentives such as premium or rate reductions for obtaining a driver's license with a biometric identifier to reduce insurance fraud.[38] Merchants may some day use biometrics to determine a person's age in order to prevent minors from purchasing alcohol or tobacco products.[39] Internet providers may begin using biometrics to limit access to adult web sites. There are endless commercial applications for biometrics beyond security uses.

Biometric security screening will be increasingly used by industry, primarily to discourage employees from stealing or selling trade secrets. Biometrics are unlikely to be implemented for

transportation security screening unless America continues to be attacked by transnational terrorists. Gloomy predictions of big brother government watching our every move will limit the use of biometrics for public security screening.

What DoD Should Do

The Department of Defense should take advantage of heightened concerns regarding transnational terrorists to institute biometric security at military base and station access points. The primary objective should be include biometric data, such as fingerprints, on existing ID and CAC cards so gate guards have a comparison tool to employ for screening individuals requesting base access. Unless DoD replaces cursory ID checks and random vehicle screening with an effective identity verification technology like biometrics and more selective and thorough vehicle inspections, guards will continue to muddle through endless processions when they could be using science to focus physical security screening on questionable persons.

> "Spotting likely terrorists among the millions of ordinary passengers is akin to finding a needle in a haystack. The dumb way to find the needle is to examine every single piece of hay. The smart way is to subdivide the haystack into clumps: one clump of pieces where the needle could not possibly be; another clump of pieces where the needle is unlikely to be, but may be worth double-checking; and the small remainder of tiny pieces where the needle may actually be."[40]
>
> Robert W. Poole Jr.

Facial recognition should be used to screen and compare individuals requesting access to military bases with a global database containing known or suspected terrorists and other lawless individuals. Terrorists can readily circumvent random security checks after minimal observation of gate guards and base security procedures. Facial recognition would arm the Department of Defense with a strong deterrent to acts of terror and enable security guards to screen for suspect persons instead of relying on traditional identification documents that are easily compromised to steal a person's identity.

---

1. Samir Nanavati, Michael Theime and Raj Nanavati, Biometrics: Identity Verification in a Networked World (New York: Wiley Computer Publishing, 2002), 9.

2. Department of Defense, DoD Biometrics: Positive Identification, <http://www.c3i.osd.mil/ biometrics/> (16 March 2003.)

3. United States Senate, S.3107: Driver's License Fraud Prevention Act (Introduced in Senate), Sponsor-Senator Richard J. Durbin (D-Il.), Introduced 10 Oct. 2002, <http://thomas.loc.gov/cgi-bin/query/F?c107:1:./temp/~c107oKfakm:e7042:> (21 Nov. 2002), 2.

4. United States House of Representatives, H.R. 4633: Driver's License Modernization Act of 2002, Sponsor-Congressman James P. Moran (D-Va. 8th), Introduced 1 May 2002, referred to the Subcommittee on Environment, Technology, and Standards 23 May 2002, <http://thomas.loc.gov/cgi-bin/query/C?c107:./temp/~c107ECNUwf> (22 Dec. 2002), 4.

5. United States House of Representatives, 1-7.

6. United States Senate, 1-8.

7. Electronic Privacy Information Center, National ID [Identification] Cards, <http://www.epic.org/privacy/id_cards/> (21 Nov. 2002), 1.

8. Legislative Director A, interviewed by author, 11 Dec. 2002.

9. Legislative Director A.

10. Judiciary Investigator.

11. Shane Ham and Robert Atkinson, Modernizing the State Identification System, An Action Agenda (Progressive Policy Institute, 7 Feb. 2002), <http://www.ppionline.org/ppi_ci.cfm?contentid=250175&knlgAreaID=140&subsecid=900017> (20 Nov. 2002), 1-2.

12. Communications Director and Legislative Director A.

13. Communications Director.

14. Legislative Director B.

15. Dibya Sarkar, "Senator readies driver's license bill," Federal Computer Week, 22 Apr. 2002,<http://www.fcw.com/fcw/articles/2002/0422/news-drive-04-22-02.asp> (21 Nov. 2002), 13.

16. Legislative Director B and Legislative Correspondent.

17. Legislative Director B.

18. American Association of Motor Vehicle Administrators, AAMVA National Standard for the Drivers License/Identification Card, 1 Jan. 2001, <http://www.aamva.org/Documents/stdAAMVADLIDStandrd000630.pdf> (2 Jan. 2003), 1-104.

19. Electronic Privacy Information Center, Biometric Identifiers, <http://www.epic.org/privacy/biometrics/> (21 Nov. 2002), 1.

20. Legislative Director A.

21. Legislative Correspondent.

22. Communications Director.

23. Judiciary Investigator.

24. Communications Director and Legislative Director A.

25. Legislative Correspondent.

26. United States Senate, 8.

27. American Association of Motor Vehicle Administrators, Problem Driver Pointer System, <http://www.aamva.org/drivers/drv_AutomatedSystemsPDPS.asp> (12 Dec. 2002), 1.

28. U.S. Government, National Strategy For Homeland Security (Office of Homeland Security, Jul. 2002), <http://www.whitehouse.gov/homeland/book/sect4-1.pdf> (10 Dec. 2002), 52.

29. Dan Balz, "Ridge Rebuts Gore Attack," The Washington Post, 23 Nov. 2002, A07.

30. Legislative Director B.

31. John D. Woodward Jr., "Super Bowl Surveillance: Facing Up to Biometrics," Rand Arroyo Center, 27 June 2001, <http://www.rand.org/publications/IP/IP209/IP209.pdf> (9 March 2003), 11.

32. "DoD Common Access Card and Biometrics Technology Demonstrations Information Paper," DoD Biometrics Management Office, 7 March 2003, 1

33. Nanavati, Theime and Nanavati, 12.

34. John D. Woodward Jr., Christopher Horn, Julius Gatune, and Aryn Thomas, "Biometrics: A Look at Facial Recognition," Rand Public Safety and Justice, 2003, 18.

35. Nanavati, Theime and Nanavati, 12.

36. Nanavati, Theime and Nanavati, 12.

37. Robert O'Harrow Jr, "Aviation ID System Stirs Doubts: Senate Panel Wants Data on Impact on Passenger Privacy," Washington Post, 14 March 2003, A16.

38 . Theodore Laven, National War College Faculty Sponsor, 9 April 2003, conversation.

39. Theodore Laven.

40. Robert W. Poole Jr., To Speed Up Airport Security, Issue I.D. Cards," Wall Street Journal, 17 January 2002, Region Public Policy Institute Web Site, <http://www.rppi.org/011702.html> (15 March 2003), 1.