Calhoun: The NPS Institutional Archive

DSpace Repository

Theses and Dissertations | 1. Thesis and Dissertation Collection, all items

2008-03

Reliability of iris recognition as a means of identity verification and future impact on transportation worker identification credential

McLaren, Simon R.

Monterey, California. Naval Postgraduate School

http://hdl.handle.net/10945/4180

Downloaded from NPS Archive: Calhoun

http://www.nps.edu/library

Calhoun is a project of the Dudley Knox Library at NPS, furthering the precepts and goals of open government and government transparency. All information contained herein has been approved for release by the NPS Public Affairs Officer.

Dudley Knox Library / Naval Postgraduate School
411 Dyer Road / 1 University Circle
Monterey, California USA 93943

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

RELIABILITY OF IRIS RECOGNITION AS A MEANS OF IDENTITY VERIFICATION AND FUTURE IMPACT ON TRANSPORTATION WORKER IDENTIFICATION CREDENTIAL

by

Simon McLaren

March 2008

Thesis Advisor:	Simson Garfinkel
Second Reader:	JD Fulp

Approved for public release; distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** March 2008	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE Reliability of Iris Scanning as a Means of Identity Verification and Future Impact on Transportation Worker Identification Credential		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Simon McLaren			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited.		**12b. DISTRIBUTION CODE**	

13. ABSTRACT (maximum 200 words)

The Department of Homeland Security is deploying the Transportation Worker Identification Credential (TWIC) to U.S. ports to help ensure only authorized individuals having undergone background checks have access to secure areas. Congress mandated the TWIC have a biometric authenticator; DHS chose fingerprints.

This thesis argues iris scanning is a better choice because of the nature of the maritime environment and because iris scanning is a more accurate biometric. This thesis also argues there are social factors affecting a biometric–enabled identification card which must be considered for the program to be successful.

To investigate the issue of biometrics and the TWIC, this thesis performed a field study of an iris scanner; a survey of biometric attitudes, and interviews with members of the PMA and the ILWU. The iris study operated the scanner in an identification mode, experiencing no false acceptances and few false rejects; however it found the scanner sensitive to sun position with respect to the subject. The pilot study of attitudes found subjects supportive of biometrics in scenarios currently requiring positive identification, but opposing them when it would create new requirements for identification. Both pilot studies were impacted by an inability to provide an incentive to study subjects.

14. SUBJECT TERMS Iris Scanning, Iris Recognition, Biometric Attitude Survey, Transportation Worker Identification Credential			**15. NUMBER OF PAGES** 147
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited.

RELIABILITY OF IRIS RECOGNITION AS A MEANS OF IDENTITY VERIFICATION AND FUTURE IMPACT ON TRANSPORTATION WORKER IDENTIFICATION CREDENTIAL

Simon R. McLaren
Lieutenant, United States Navy
B.S., Adams State College, 1998

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN COMPUTER SCIENCE

from the

NAVAL POSTGRADUATE SCHOOL
March 2008

Author: Simon McLaren

Approved by: Dr. Simson Garfinkel
Thesis Advisor

J.D. Fulp
Second Reader

Peter Denning
Chairman, Department of Computer Science

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The Department of Homeland Security is deploying the Transportation Worker Identification Credential (TWIC) to U.S. ports to help ensure only authorized individuals having undergone background checks have access to secure areas. Congress mandated the TWIC have a biometric authenticator; DHS chose fingerprints.

This thesis argues iris scanning is a better choice because of the nature of the maritime environment and because iris scanning is a more accurate biometric. This thesis also argues there are social factors affecting a biometric–enabled identification card which must be considered for the program to be successful.

To investigate the issue of biometrics and the TWIC, this thesis performed a field study of an iris scanner; a survey of biometric attitudes, and interviews with members of the PMA and the ILWU. The iris study operated the scanner in an identification mode, experiencing no false acceptances and few false rejects; however it found the scanner sensitive to sun position with respect to the subject. The pilot study of attitudes found subjects supportive of biometrics in scenarios currently requiring positive identification, but opposing them when it would create new requirements for identification. Both pilot studies were impacted by an inability to provide an incentive to study subjects.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ABBREVIATIONS

AAPA	American Association of Port Authorities
ATSA	Aviation Transportation Security Act
DHS	Department of Homeland Security
DoD	Department of Defense
FNMOC	Fleet Numerical Meteorology and Oceanography Center
FPR	False Positive Rate
FRR	False Rejection Rate
HIIDE	Hand-held Interagency Identity Detection Equipment
ILWU	International Longshore and Warehouse Union
IR	Infra-Red
IRB	Internal Review Board
MTSA	Maritime Transportation Security Act of 2002
NIST	National Institute of Standards and Technology
OCR	Opinions Research Corporation
PIER	Portable Iris Enrollment and Recognition
PMA	Pacific Maritime Association
RFID	Radio Frequency Identification Device
TSA	Transportation Security Agency
TWIC	Transportation Worker Identification Credential
USCG	United States Coast Guard

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I express my most sincere thanks to:

My wife for her support during the process of this thesis, being willing to listen to endless comments about biometrics and surveys, and her help in editing and proofing this document.

Professor Simson Garfinkel who, while he would likely say he was just doing his job as an advisor, provided an amazing amount of direction, support, editing, questions and insight throughout the entire research and writing of this thesis.

SecuriMetrics, the manufacture, was also kind enough to lend us a PIER 2.3 for the duration of the experiment. This reduced the costs associated with the experiment and provided some additional flexibility for other un-anticipated expenses that might be encountered later on during the course of the experiment, survey or thesis research. We desire to express our thanks to the SecuriMetrics Company for their willingness to allow us to use the PIER 2.3 without charge.

Tim Johnson of SecuriMetrics for taking the time to train the thesis author in the use of the PIER 2.3 device.

James Albers – VP, Government Operations – SecuriMetrics for his help in coordinating the legal issues in the lending of the PIER 2.3

Ed Hughlett (Manager Northern California Area Safety and Health – Marine Terminal Corporation) and Kevin Kirk (Assistant Director, Security & Accident Prevention, Pacific Maritime Association) for taking time to provide a great deal of insight to many of the social and technical issues surrounding the practical implementation of the TWIC.

Ed Capizano (Union representative for the International Longshore and Warehouse Union Local 91) for his willingness to speak openly and frankly about the privacy concerns the ILWU members have with the TWIC program.

CDR A.J. Reiss Executive Officer of Fleet Numerical Meteorology and Oceanography Center for being so cooperative in opening up his command and facilities to support the field experiment.

A special thanks to the four volunteer operators of the iris scanner for being willing to act as operators for the week of the field experiment of the PIER 2.3 Device.

I. INTRODUCTION

This thesis examines how iris scanning could improve the Transportation Worker Identification Credential (TWIC) program. This thesis conducted two pilot studies: a field usability study of the SecuriMetrics PIER 2.3 Iris device and a study of biometric attitudes. Both studies were hampered by the inability to provide adequate incentives to obtain greater numbers of volunteers. Nevertheless, the conclusions of both studies were consistent with other research in this area.

Iris scanning has the potential, if implemented correctly, to drastically improve the accuracy of identification of workers in security sensitive positions. Applied to transportation workers at U.S. ports, iris scanning could considerably reduce the chances of an unauthorized individual gaining access to sensitive areas, making the shipping port less vulnerable to attack.

Iris scanning is a "stand-off" biometric, meaning that it requires no physical contact between the subject and the iris scanning device. The accuracy of iris scanning appears to be vastly superior to other forms of biometrics. Daugman claims that with millions of scans performed, there have been zero false matches with iris scanning [9]. Even if this is an overstatement of the accuracy of iris scanning, there is no doubt that iris scanning is vastly superior to the other methods of "stand-off" biometrics, including facial recognition and gait recognition which have traditionally had significant error rates [41].

The Transportation Worker Identification Credential (TWIC) program will require the use of biometrics at U.S. shipping port facilities for identity verification. Great care must be taken in the shipping port environment to minimize the time required to collect and process a biometric if they are to be used for identification purposes on a daily basis. Any method that would slow the entry or exit of dock workers or truckers in or out of the port would have an impact on the efficiency of the port itself, resulting in higher prices of all shipped goods.

Any major disruption to the normal operation of U.S. port facilities would likely have a noticeable impact on the U.S. economy. For example a 2002 labor dispute which led to a 10 day shutdown of West Coast port operations cost the U.S. economy an estimated $1.5 billion daily [3].

Mr. George Cumming, the Director of Homeland Security for the Port of Los Angeles, in his May 2006 testimony before the Senate Committee on Commerce, Science and Transportation, noted that he expects the amount of commerce at the Port of Los Angles will continue to grow at 20% per year, and that the industry as a whole will double by 2020 [5].

Current plans are to use fingerprints as the biometric to validate the identity of TWIC card holders. Fingerprint scanners are likely to experience significant challenges in the unique conditions that the marine environment and a gated facility present. Some of these challenges could be addressed through the use of iris recognition and the adoption of very recent product developments in iris technology.

Iris scanning has the potential to allow the collection of a biometric for identification or verification purposes at a moderate distance and even through wind-shields or windows of vehicles. This might significantly reduce the impact that the adoption of biometric identification requirement will have on U.S. shipping ports, by allowing the collection of the iris scan without requiring the driver to get out of the vehicle and maybe even without stopping.

Recent developments in iris scanning are moving this biometric technology quickly to a point where iris scanning may be the biometric of choice to achieve both high rates of accuracy and high speed of collection of a biometric for identity establishment or verification.

A. BIOMETRICS IN THE POST – SEPTEMBER 2001 ERA

The attacks of September 11, 2001 left the Nation in shock and made it clear that the freedom of movement Americans enjoy in the United States may come with a price — vulnerability. In a society that prides itself in the ease at which its citizens are able to

travel and a low level of government involvement in the daily lives of its citizens, we became very aware of how those freedoms may provide our enemies opportunities to exploit.

That day forced America to ask if the freedom of movement and levels of privacy its citizen enjoy are worth the risk that freedom and privacy come with. Some argue that those attacks and the lives lost that day are the price that must be paid for those freedoms. Others argue that the price is too high and that privacy should not be guaranteed at any price, especially at the cost of thousands of civilian lives. Some would go so far as to say the only reason an individual seeks anonymity is to do things that are illegal and that any law abiding citizen should not have any fear of the government knowing what they are up to and where they have been. This thesis examines how the public views biometrics and looks for commonalities in what uses of biometrics are deemed acceptable and where the use of such technology crosses that line of the public's perceived right to privacy.

B. TRANSPORTATION WORKER IDENTIFICATION CREDENTIAL

1. Origins of the Transportation Worker Identification Credential

The attacks of September 11, 2001 also brought great attention to the fact that some U.S. centers of transportation were at risk. It pushed those concerns to the very front of the agenda of the U.S. Congress. Shortly after the attack, Congress passed the Aviation Transportation Security Act (ATSA) and the Maritime Transportation Security Act (MTSA) in an effort to address two vulnerabilities. These Acts direct today's Department of Homeland Security to secure the U.S. Airports and Shipping Ports. Both of these Acts require the use of background checks on all personnel needing unescorted access to secure areas of either U.S. airports or U.S. shipping facilities. They also created the requirement that once cleared, these individuals will be issued identification that would be difficult to counterfeit, difficult to alter, and biometrically verifiable.

The DHS chose to move forward with its efforts to provide the newly required identification at U.S. shipping facilities first. Because of the economic importance of maritime shipping facilities to the overall U.S. economy, anything that might impact the

efficiency of these ports and their operations has potential to have a significant impact to the U.S. economy. The decisions surrounding which form(s) of biometric verification should be used to achieve the required verification should take into account the potential adverse impact the biometric collection method will have on the shipping facilities.

The Transportation Worker Identification Credential (TWIC) program is intended to help meet the requirement of those laws by providing a biometrically verifiable identification token that is cryptographically protected from counterfeiting and alteration [11]. The idea is straight forward: if an individual passes the background screening and if it can be verified that the TWIC card itself has not be altered and that the holder is the individual identified on the card, then one can be reasonably certain that the individual holding the card is trusted to have access to whatever the TWIC card provides. This is intended to increase the security of the transportation infrastructure of the United States.

The TWIC is intended to be issued to all personnel who need unescorted access to the secure areas of U.S. shipping ports, some vessels, and eventually to U.S. airports as well. A secure area is any area beyond the gate to the port facility. DHS has also identified some ships as having "secure areas" and workers on these ships will also need to have TWIC cards to maintain unescorted access to these areas. The TWIC will be required for all dock workers (longshoremen), truckers who transport freight in and out of the ports, delivery drivers (UPS, vending machines, food, etc.), Port Authority personnel, and those who work on the ships and require access to secure areas of the ships and so on. In all, DHS estimates that over 770,000 personnel will eventually need to be issued a TWIC.

C. IMPLEMENTATION ISSUES

The TWIC card itself is intended to serve as a model for the form of identification mandated by Homeland Security Presidential Directive-12 (HSPD-12) [11]. The TWIC program will eventually require the use of a biometric card reader. In January 2007, the TSA and USCG issued the first TWIC rule that mandates that workers who require unescorted access to secure areas of maritime facilities be enrolled in the TWIC program and that procedures be changed to ensure those seeking unescorted access have a valid

TWIC card [57]. However, neither the TSA nor Coast Guard requirements mandated any specific biometric card readers. This was in direct response to the request for public comments on the draft of its first rule. In particular the American Association of Port Authorities (AAPA), the group who owns and operates most U.S. shipping facilities, noted that most biometric systems have not been tested in a maritime environment and that these systems should be tested and certified for use in such an environment before being required [57]. The problem is that very few biometric readers have been tested in the maritime environment.

In its April 12, 2007 report to the U.S. Senate, the TSA noted that the industry would face challenges with implementation of TWIC. In the test and pilot programs very few sites tested the biometric card readers that are required by the MTSA. This provided very little information on how this sort of readers would handle the "dirt, salt, wind and rain" of the maritime environment [3].

Challenges are also sure to arise when biometric readers are installed on shipping vessels which could again prove to be a unique environment with no tests of biometric readers having been conducted in this environment either [4]. Shipboard readers will present a challenge of "reach-back" over wireless (most likely satellite communications) channels; and there has been no test of how these connections will be made.

D. IRIS SCANNING IN A PORT ENVIRONMENT

Ensuring the accuracy of identification and biometric verification is of substantial interest to the security of the United States. It is in the economic best interest of the nation to ensure that this process of checking IDs and physically obtaining a biometric to establish or confirm the identity of the identification holder be made as efficient as possible.

In a telephone interview, Mr. Cummings, the Director of Homeland Security for the Port of Los Angeles, indicated that the use of the TWIC card with the requirement for a biometric verification of the holder would be of great concern at the port's entry. While the current requirement is that a guard must visually verify the identity of the holder, once the biometric check is enforced, the increased processing could cause considerable

delay and backup of traffic attempting to enter the port facility. He also indicated that while the current direction of the TSA was to use fingerprints, that given the limited experience anyone had with fingerprint scanners in a maritime environment that the dependability of the scanner was also of great interest.

E. TWIC TO USE FINGERPRINTS AS BIOMETRIC

1. Decision to Use Fingerprints as Biometric of Verification

The TWIC Final Rule issued on 25 January 2007 made fingerprints the biometric to be used by the TWIC program. The use of fingerprints will facilitate the background check process as fingerprints can be matched against the FBI criminal databases and the fingerprint templates will be stored directly on the TWIC Card [57].

F. IRIS SCANNING AS AN EFFICIENT ALTERNATIVE

1. Why Iris Scanning Might Make More Sense

Iris scanning as a biometric makes more sense for the TWIC given the requirements for high speed and operation in the hostile maritime environments. The big advantage of fingerprints — compatibility with existing biometric databases — is not relevant here. With fingerprint scanners the subject must make physical contact with the scanner for the print to be acquired. In the gated facility scenario in which the TWIC will be used, this means the subject who is driving the vehicle must bring the vehicle to a complete stop. The subject must then physically reach outside of the vehicle to make contact with the fingerprint scanner, or the fingerprint scanner must be moved into the vehicle to facilitate the physical action of the fingerprint scan.

The port environment also provides for a couple of scenarios that could make fingerprint scanning more challenging than usual. The port environment includes bodies of water. While it is not normal for workers at a port to be in the water, workers could

still experience a common side effect of working in wet environments: wrinkled or shriveled fingers. Here again iris scanning would prove far more reliable if wrinkles cause issues with fingerprint scanners.

Fingerprint scanners also require that the subject make physical contact with the fingerprint scanner itself. This brings up issues of sanitation due to the constant contact by multiple individuals [54]. Port facilities tend not to be the cleanest environment. Shipboard workers, especially those who work on the ship power-plants (engines) are exposed to grease or other petroleum based contaminants. This will certainly present a challenge to the reliability of fingerprint scanners.

2. The Promise of Iris Scanning at a Distance

Here is where iris scanning may hold the most promise. "Iris-at-a-Distance" is the set of technologies that allows an iris scanner to acquire an iris scan of a subject at a considerably greater distance than the current norm for an iris scanner. Some research in this area has shown potential for this at distances of up to one meter, even while the subject is moving [21][22][26]. The Sarnoff Corporation has introduced an indoor iris scanner that is capable of capturing irises from individuals walking at distances of up to three meters [24]. Just in November 2007, Sarnoff announced a "drive-through" iris scanning system [25].

If iris-at-a-distance technologies can become financially practical this could potentially eliminate the requirement for a vehicle driver to come to a complete stop at a gated facility. Policy is not likely to allow for "roll-by" entry through a gate. However, iris-at-a-distance technologies could eliminate the need for most drivers to dismount their vehicle to provide a biometric scan, while making the scan as easy as looking in a particular direction.

G. PRIVACY CONCERNS OF TWIC PROGRAM

There are privacy concerns with the TWIC program, just as there are with any program that requires collection of large amounts of personally identifiable information about people. The DHS Inspector General released a report [1] that highlighted some of

these concerns, which are one of the reasons that the program has been delayed [2]. One concern is that the TWIC program does not have any data retention policies governing the length of time data is stored or any procedures for removing data from TWIC databases when it is no longer needed [2].

A second area of research in this thesis is the current public opinion toward the acceptability of biometrics in some specific scenarios. The TWIC program will likely move forward using a biometric scan for verification without any roadblocks caused by general public concern over biometric use because it does not apply to the general public. However, it will need to address the opinions and mistrust of the workers who must be issued the TWIC, or else workers may seek to subvert the program.

The TWIC is intended to meet the requirements of HSPD-12 which mandated the use of "secure and reliable form of identification" [11] to all government employees and contractors. The Federal Information Processing Standards Publication 201 provides the standard for how the HSPD-12 forms of identification should be implemented and requires the use of biometrics [13]. Given the large number of individuals HSPD-12 will effect (all U.S. Government employees and contractors), and the FIPS-201 requirement for the use of biometrics, the experience of the government with the TWIC may be directly applicable to some future HSPD-12 systems.

Another specific challenge for the TWIC card and biometrics comes from the unionized longshoremen who work at the port facilities on the West Coast. The union sees the TWIC as a method for the Pacific Maritime Association (PMA) to better track the hours being worked by the longshoremen. One requirement of the MTSA is that port operators should know who is in their port at all times [17]. If the TWIC card is used to facilitate this, then undoubtedly there is a record kept of all entries and exit to the facility along with times of entry and departure. It is not a far leap of the imagination that this information could be used to establish a "time-clock" of sorts for dock workers.

The union ensures that union members will be paid for a full eight hour work day even if the job they do for the day does not take the full eight hours [14][61]. Some job in particular require the longshoreman to be on the job to perform his assigned tasks early

in the day and again late in the day, with no tasks being required of this worker for large portions of the time in between. This is an employment issue rather than one of security, but it shows some TWIC users may seek to subvert the system for reasons other than attacking port security.

H. PRIVACY CONCERNS AND BIOMETRICS

In general, concerns about privacy and biometrics include: that the data will be used only as advertised, a lack of trust by the general population that the data will be properly protected from unintended disclosure and the possible physical risks that the collection of biometrics might create, to name a few.

A 2001 survey showed that there are some situations in which the public is very comfortable with biometrics being used. The potential use of biometrics for screening individuals seeking access to military bases and laboratories and to screen individuals desiring to purchase a fire arm, are two examples where the public is comfortable. People also seemed to be fine with the idea of collecting biometrics from convicted criminals [15]. The survey also showed that the public appears to be more concerned that the data collected for a large biometric system will end up being used for more that originally intended than they are with the actual methods for biometric collection.

More recently TRUSTe conducted a survey that showed 82% of Americans are in favor of biometric identification on passports. Seventy-five percent of Americans think biometrics are a good idea on driver's licenses and almost seventy-three percent think biometrics would be a good addition to social security cards [20]. This would seem to indicate that individuals seem more open to the use of biometrics when it comes to protecting their identity.

I. RELIGIOUS BELIEFS MAY LEAD TO CONCERNS

Some people are opposed to the use of biometrics on religious grounds. The majority of these objections seem to be based on Revelations 13:16-18, which warns of a future in which the people of the world will be forced to wear the "Mark of the Beast" in order to buy or sell, or to obtain food.

For example, while visiting SecuriMetrics/L1-Securities, the manufacture of the Iris Scanner used the field experiment, I had a passing conversation with a visitor who had stopped by the L1 facilities. When I ask very casually what he thought about the technology that L1 manufactured, he responded, "This technology is the Mark of the Beast." This same connection was drawn by three respondents of the survey that we performed, even though there was no mention of the Mark or Revelations on the survey.

While it is doubtful that iris scanners are truly the fulfillment of prophecy, the association between the two appears to be present in some people's minds. Peter de Jager notes that, regardless of how irrational beliefs like that above are or seem to be to someone else, they are beliefs for some, and must be considered and addressed if change is ever to occur [16].

J. BIOMETRICS ALONE DO NOT SOLVE ANYTHING

All the technology can do is to help ensure we limit access only to individuals who have been deemed trustworthy [18][19]. A key to the success of the TWIC program providing improvements to the security of U.S. shipping port will be the ability of the TWIC program to enroll individuals needing TWIC cards into the program and issuing TWIC cards to them. Far more important will be the screening process and criteria that will be used to ensure only "trustworthy" individual receive a TWIC card. The current guidelines would disqualify anyone who has been convicted of a felony within the last 7 years, or release from incarceration for a felony in the last 5 years [17]. One question that will affect the TWIC card's success is whether or not these criteria successfully allow the government to identify individuals who represent a threat to the security of the Unites States, while not preventing individuals who have a rough past but who are not a terrorist threat from pursuing good paying jobs as longshoremen. Based on interviews conducted for this thesis, it is clear that if the TWIC program is seen as disrupting livelihoods while not improving overall security, it will not be successful because the intended enrollees will work to subvert it.

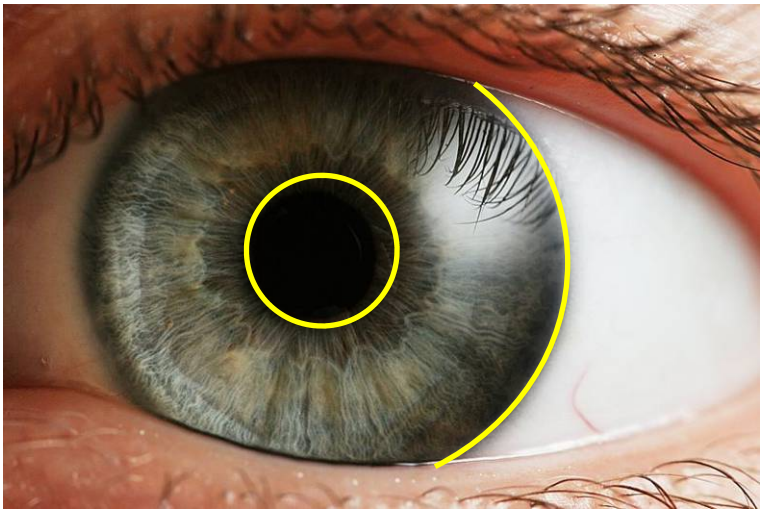
II. IRIS SCANNING: TECHNOLOGY AND USES

A. INTRODUCTION

1. Iris Recognition, Technology and History

In 1993 John Daugman introduced iris scanning as a new biometric. He did so by answering three questions. 1) Were there enough degrees-of-freedom in the iris to use it to singularly identify and individual (there were), 2) was it possible to derive an algorithm that could efficiently create a match-able iris template form an image (it was) and 3) could that algorithm render a match decision with high statistical confidence within a reasonable amount of time and with reasonable computing resources (it could) [8].

Daugman's technique uses a video camera to acquire the iris image. His algorithm first determines if an iris is in the image and if so, then identifies the iris position. The basic process uses the fact that the white of the eye is much whiter than the iris itself to establish the outer edge of the iris in an image (outer line). The inner edge of the iris is then established using the fact that, while the pupil might not be much different in color form the iris itself, (especially in the case of dark eyes) the pupil is a homogenous color while the iris is less homogenous (inner line).



As an aside, Daugman notes that the pupil itself changes diameter nearly constantly even in conditions of steady illumination and that this property of the eye can be used to create a "liveness" test of a video image being used to test an iris[8].

Once acquired, iris images are passed through 2-D Gabor filters to produce a binary "iris code" of the image. This results in a 256 byte code or "template" for the iris. Even in 1993, the process of calculating this code took just 100 msec on a standard computer.

The original iris code algorithm produced a 256 byte code for each iris. The size of the code was chosen because 256 bytes was consistent with the amount of data that could be stored in the magnetic stripe of an IS-7811 credit/debit card[8]. While the length of the iris code appears to have been driven by the technology available for an anticipated market of the iris algorithm, a key to iris scanning was to achieve a constant length code for all irises. Daugman explained that this property of fixed-length lends itself to both the "speed and reliability of iris recognition decisions." He also notes that the variability in the length of the output of a representation in fingerprints has been a complicating factor in the use of that technology for identification [8].

One of the greatest claims of Daugman's study established "the likelihood of two iris codes from different irises agreeing completely by chance is roughly one in 2^{173}, or approximately 10^{-52} [8]." Yet over the years, this claim has help up.

Once a template has been acquired for a subject it will need to be entered into an iris template database. Here it will remain, waiting to be matched against another template.

To match an iris the system must first capture an image of the iris in question. The image is run through the same conversion process to produce a second 256 byte iris template. This new template is then used to search for a "match" in the iris template database that contains known irises. Here a match is a statistical match. Two images of the same iris are not likely to produce the same 256 byte template, due to variations in the images themselves. A match is defined as finding an iris template in the iris template database that matches "close enough".

Daugman received a patent for his algorithm in March 1994 [27].

The match decision is made by computing the Hamming Distance between two samples. The Hamming Distance is the percentage of bits of the known iris code and iris scan being tested that do not match [9]. If an iris scan matches 80% with a known sample then its Hamming Distance would be 0.20 for that iris code pair.

2. Basic Description of Iris Match

Much as your signature is never quite the same, templates of the same iris will differ to some degree due to variations in the "configuration" of the eye, differences in position of the camera and possibly due to lighting conditions at the time. The eye "configuration" refers to the size of the pupil (due to lighting or other physical causes that would cause to dilate or constrict), the position of an individuals eyelids (which may occlude part of, or expose more of the iris than in the original image) or eyelashes or hair occluding a part of the iris. The image may also be slightly distorted by the use of eye glasses, sunglasses or contact lenses.

The new iris template is then run in an exhaustive search of the template database looking for a match that is close enough to call it a match. Here the templates are compared on a bit by bit basis to look for correlation. One might simply XOR the two templates together and count the number of 1's left over, divide that by 2048 (256 bytes * 8 bit/byte) yielding a simple percentage difference between the two templates. This percentage difference is what Daugman describes as the Hamming Distance between two templates.

Daugman derived a table of Hamming Distance values and the corresponding odds of a false match (False Acceptance Rate) and false reject (False Rejection Rate). He suggests that the Hamming Distance required to statistically result in a match can be tailored to the given application that an iris recognition system is going to employed in. This means that an organization can choose and set the tolerance they are willing to accept for their iris system. For those who are more concerned about the threat represented by allowing a false match, the Hamming Distance can be set to a higher level

of tolerance, meaning it requires a greater percentage match between the known sample and test iris code to result in a "match" [9].

Higher chance of False Reject ↑

HD Criterion	Odds of False Accept	Odds of False Reject
0.25	1 in 13.5 billion	1 in 1,490
0.26	1 in 2.04 billion	1 in 2,660
0.27	1 in 339 millin	1 in 4,850
0.28	1 in 60 million	1 in 9,000
0.29	1 in 12 million	1 in 17,100
0.30	1 in 2.4 million	1 in 32,800
0.31	1 in 603,000	1 in 64,200
0.32	1 in 151,000	1 in 128,000
0.33	1 in 39,800	1 in 260,000
0.34	1 in 11,500	1 in 536,000
0.35	1 in 3630	1 in 1.12 million

↓ Higher chance of False Accept

Table 1. Performance Tabulated as Error Probabilities for several Decision Criteria or Various Hamming Distance (From [8])

Daugman states that the process of the statistical matching algorithm itself, when comparing a sample iris code to one that has been previously stored, will result in a match or a non-match. This leads to one of four possible outcomes:

Acceptance of Authentic (AA): a result of "Match" on the authentic iris. More simply put, the iris template being tested against (template A) is a statistical match to the template (template B) in question. Here, template B is in fact a template created from the same iris that produced template A at some earlier point.

False Acceptance (FA): a result of "Match" on an imposter iris. Here the iris template in question (template B) is found to be a statistical match to a template previously (template A). However, in this case, templates A and B were generated from two different irises.

False Rejection (FR): a result of "non-match" on the authentic iris. In this case the iris template in question template B is not found to statistically match to template A. In this case, templates A and B where generated from the same iris.

Correct Rejection: a result of “non-match” on an imposter iris. Here the iris template in question (template B) is not a statistical match to the template it is being compared to (template A) and in fact templates A and B were generated from two different irises.

In practice, a single acquired template is compared against many templates that have been previously collected and stored in a template database. The template in question is compared to templates in the database until either a statistical match is found or until all templates in the database are exhausted.

Daugman showed that with a circa-1993 desktop computer it was possible to perform exhaustive searches of an iris database at a rate of about 4,000 templates per second. He theorized that a relatively inexpensive specialize circuit would have been able to search nearly 160 million iris templates per second exhaustively [8].

By 2004 [9] the speed at which the iris matching algorithm would run had increased substantially. Today we estimate that a 300-MHZ processor, typical of handheld computers and cell phones, is able to compare 100,000 iris templates per second; and on a typical 2-GHz desktop, comparisons can be run at a rate in excess of 580,000 matches per second. Given the estimated U.S. population of approximately 303,230,000 [10], it would be possible for this server configuration to do an exhaustive comparison of the entire U.S. population in approximately nine minutes (18 minutes if both left and right eyes of the population are compared). Since exhaustive search is inherently parallel, nine computers could reduce the search to one minute; 90 computers could reduce the search time to six seconds. Of course, no such database of biometrics exists today, so such numbers are necessarily theoretical.

Until recently, iris scanners have been used almost entirely in controlled environments such as an office space. This environment provides some level of predictability of environmental factors, in particular the direction and level of light intensity of the ambient light that could have an effect on the accuracy of the iris scanner. To overcome the limitation that light levels may present, manufactures have incorporated infra-red illuminators in some iris scanners.

Infra-red illumination is used as iris detail is best captured in the infra-red wavelength. At this wavelength (700-900 nm) the effect of dark eye color masking the detail of the iris are eliminated [9]. However; iris recognition has been shown to be possible using still images taken in the visible wavelengths as well [40].

3. False Accepts vs. False Rejects

As noted above, the Daugman algorithm can have its matching criteria set or adjusted to meet the need of the application to which it is being applied. This provides the end customer or equipment manufacturer the ability to customize the system to err on the side of security where the cost of a false accept is deemed very high and the customer is therefore willing to accept a significant number of false rejects. Or the system can be set up for the other extreme where having the occasional false identification is deemed acceptable given that the systems does not produce many false rejects.

One can see where the first scenario fits well with applications that require high degrees of security, and where the ability to screen out an imposter is far more important than the inconvenience created when the system falsely rejects an acceptable individual. In these cases procedures can be put in place to handle the occasional false reject.

A scenario where the occasional miss-identification might be acceptable would be where the goal is tracking the frequency that individuals perform a certain action. Port security is probably such an application.

4. Identification vs. Verification

Biometrics offer the ability to match an individual against a pre-obtained biometric template. This can be done in one of two methods: to either establish someone's identity, or to simply verify their identity.

a. Using Biometrics to Establish Identity

With identification (or identity establishment) the individual in question does not need to provide any claim of who they are. In this case a biometric measurement is collected from the individual. That biometric measurement is then

converted into a template. That template is then compared to templates in a database (exhaustively or with more intelligent methods). If a match is found and the matching template is tied to an identity (which usually takes place during a registration process) then the individual who provided the template in question is determined to be the individual indentified in the database.

On the plus side in this scenario, there is no dependence on the subject to provide any claim of identity. This is a plus with a subject who is intentionally attempting to be misleading or who is unable to provide an acceptable claim of identity. (Think of an individual using a credit card without any form of picture ID.)

On the downside: Identity establishment often requires an exhaustive search of a biometric template database. Depending on the size of the database or more precisely the number of templates that it must be compared to and the speed at which these comparisons can be made this can require considerable resources to perform.

b. Using Biometrics to Verify Identity

For identity verification the process begins very similar. A biometric measurement is obtained from the individual in question. However, in this case the individual also provides some manner of claimed identity. This could be as simple as stating their name or as complex as providing a "Smart Card" that contains their identity and key into a biometric database. The biometric measurement collected is then turned into a template to again be used for comparison. However, since the individual in question has already provided us a claimed identity, in this case the system would retrieve only the template of the individual the individual has claimed to be. Here we will only compare the template collected from the individual against the template in the biometric database tied to the claimed identity. If we have a match, then we have confirmed the identity of the individual. This is similar to how an ATM card and PIN works. The ATM card is the claimed identity and the PIN is used to verify the claimed identity.

One advantage of verification is that, by limiting the number of templates that must be searched in order to arrive at a conclusion about the validity of the claimed

identity, the verification process can be performed faster on less expensive hardware. This can save resources and results in a much faster match result.

One disadvantage of identity verification is that if the claimed identity is incorrect, then there is no determination of who the imposter is. This may be fine if the only goal is to not allow authorized individuals access to some protected resource, but falls woefully short if there is a need to determine who the imposter is. (Of course mismatches could be recorded and identified later.)

B. CURRENT STATE–OF-THE-ART

Current iris technology can be grouped into a few different categories. One could separate them by whether the scanning unit is fixed in location or mobile, whether the subject being scanned must be relativity still or can be moving or even by the distance the iris scanner must be from the subject to obtain a clear image. This section reviews examples of scanners that fall into three distinct groups: Fixed or mounted iris scanners, handheld scanners, and iris scanners that can acquire iris images from a reasonable distance.

1. Fixed or Mounted Scanners

Fixed or mounted iris scanners have been the most common category of iris scanners. These scanners require the subject to bring their iris into close proximity of the scanner itself. Close proximity here is approximately 6-12 inches between the scanner and the iris whose image is being captured. A few commercially available examples of this sort of scanner are:

Figure 1. Frequent Flyers program at Schiphol Airport in the Netherlands uses the LG IrisAccess-2200. (From [29])

Fixed or mounted iris scanners are being introduced into many applications. One of the big advantages the fixed scanners provide is that they can be used in an unmanned setup when subjects are cooperative. This has made this particular category of scanners useful in office building access and airport settings where the environment tends to be more controlled. The systems are generally connected to a central template database as the number of registered users tends to be high.

2. Handheld Scanners

Handheld iris scanners provide the ability to utilize them in applications that require the iris scanner to be mobile. The devices that are available commercially in this category tend to be ruggedized as the U.S. military is one of the larger customers. These devices tend to be more suited for the outdoor environment or simply environments where there is less control over the conditions. A couple of examples:

Figure 2. U.S. Marine Corps Sgt. A.C. Wilson uses a retina scanner to positively identify a member of the Baghdaddi city council prior to a meeting with local tribal figureheads, sheiks, community leaders and U.S. service members deployed with Regimental Combat Team-7 in Baghdaddi, Iraq, on Jan. 10, 2007. Wilson is attached to the 4th Civil Affairs Group. (From [50])

The SecuriMetrics PIER 2.3 (Portable Iris Enrollment and Recognition Device) is the handheld device used in the field experiment in this paper. This device is lightweight and simple to use. This particular device captures iris images at a distance of approximately 4-6 inches [49].

The HIIDE (Hand-held Interagency Identity Detection Equipment) is a multi-modal scanner with an iris scanner, a fingerprint scanner, and a camera for facial recognition, allowing the operator to utilize more than one biometric to establish the identity of an individual. The HIIDE allow a subject in the field to be matched against multiple databases containing different kinds of biometric templates. Alternatively, the device allows subjects' irises, fingerprints and facial templates to be collected in a single registration; thus allowing the templates to be interoperable with different systems.

The HIIDE image capture distance is approx 8-10 inches; the systems can store approximately 10,000 biometric portfolios (2 iris templates, 10 fingerprints and a facial image).

3. Iris Recognition on Cell Phones

In November 2006, OKI announced a successful development in Iris Recognition middleware software for use on cell phones [55]. This development has the potential to reduce the cost of iris image capture devices, making iris scanners ubiquitous.

Figure 3. OKI's mobile-oriented iris recognition middleware (OKI Electric Industries)

4. Iris at a Distance

The last category is that of scanners that can acquire the iris image at a distance. This category of scanner opens the door to even less physically intrusive iris image capture. Current scanners in the group are able to capture iris at a distance of up to 10 feet away[24][25].

C. CURRENT DEPLOYED USES

Iris scanners to date have found themselves used almost entirely in controlled environments such as an office space. This environment provides some level of predictability of environmental factors; in particular, ambient light levels that could have an effect on the accuracy of the iris scanner. To overcome this limitation, manufacturers have incorporated infra-red illuminators in some iris scanners.

More recent applications have moved iris scanners into less controlled environments. In Iraq, the U.S. military is using iris recognition devices like the PIER 2.3 to provide identification for the purpose of screening Iraqi army recruits. This application is conducted in much less controlled environments [51], although no information has been made publically available about the performance of the PIER 2.3 in Iraq.

1. Border Control

In 2001, the United Arab Emirates (UAE) Ministry of Interior launched an iris recognition system to check visitors and individuals on work visas, against a database of UAE inmates and expellees. The system uses iris cameras made by LG and a networked server infrastructure system made by Imad Malhas of Iris Guard [53]. The expellee database has grown to nearly one million [29]. Visitors' irises are run against an exhaustive search of the database to look for matches. The UAE averages about 6,000 visitors or 12,000 irises per day, which equates to approximately 10 billion comparisons per day [29]. So far, roughly 7.5 million exhaustive searches equating to over 7 trillion comparisons have been made. The system has matched over 73,000 individuals seeking entry to the UAE that are on the watch list. All matches have been confirmed via other records. The UAE system is the largest iris recognition system in use today [29].

2. Refugee Assistance and Fraud Prevention

Iris scanning systems are being used by the United Nations High Commissioner for Refugees (UNHCR) in Afghanistan and Congo to ensure that returning refugees are provided assistance, and that individuals are unable to fraudulently seek assistance more than once. As of May 2005, nearly 500,000 people had been enrolled in the system with expectations of an additional 300,000 by the end of 2005. In this application, UNHCR experienced failure to enroll rate of 0.42%. The iris system helps to ensure that cash grants are distributed only to first time applicants [35].

Figure 4. The United Nations High Commission for Refugees administers cash grants to refugees returning into Afghanistan from surrounding countries after the fall of the Taliban, using iris patterns in lieu of any other forms of identification. More than 350,000 persons have so far been processed by this programme using iris recognition. This picture shows the Takhtabaig Voluntary Repatriation Centre, on the Pakistan-Afghan border. (From [29])

3. Airport Security

In recent years iris scanning has been used in both airport frequent flyer programs and airport security. Most of these programs are voluntary but offer volunteers the ability to bypass at least some elements of airport security and thereby removing or reducing a common hassle of air travel. A few examples of these programs are:

a. Privium at Schiphol Airport Amsterdam Netherlands

In October 2001 the Schiphol Airport in the Netherlands introduced a frequent traveler program called Privium. The program is open to anyone with a valid passport from one the European Economic Area countries and Switzerland. The program allows travelers to register in advance and then again bypass the long customs and

immigration lines at airports when entering the country. A total of 18 airlines participate in the program. The system reduces the time required to gain approval to cross the border to 15 seconds. Participants must be at least 1.5 meters tall and be able to use the iris scanner without assistance [28].

In December of 2006 Indonesia introduced the Shaphire program to the Jakarta airport, a program similar to that of the Privium program [32].

Heathrow Airport in London launched Project IRIS (Iris Recognition Immigration System) in June of 2005. In the Pilot Review Report the UK Immigration Service Home Office stated that the program's FTE rate was 1.47. The average time to pass through the iris scanning barrier was just under 15 seconds, with 79% of attempts being complete in under that time. The fixed enrollment time was 256 seconds. No false accepts were experienced during the pilot program. The false reject rate was 3.57%; however, it was not possible to determine how many of those rejections were due to non-enrollees attempting to use the system [31].

The UK government has expanded the program to include terminals at Heathrow, Manchester, Birmingham and Gatwick airports [31]. According to the official IRIS website there are currently 150,000 enrolled travelers and the system has successfully performed over 750,000 automated border entries [31]. Enrollees are required to have a valid passport and disabled passengers are encouraged to be understanding if the system will not accommodate them [31].

The Frankfurt Airport BioP II trial had far less impressive results. In this pilot program the testers experienced a false accept rate of 0.0023%. The study noted that false rejections seemed to decrease the more often subjects used the iris system. Frankfurt Airport chose to use fingerprint scanners to expedite travelers at the conclusion of the trial. The iris scanner used for this trial did not perform automatic eye detection [34].

Figure 5. The system above was used during the trial Frequent Flyers program at Frankfurt/Main Airport but has been discontinued with the decision to use fingerprints for identification instead. (From [30])

The United States has also launched a Registered Travelers program which provides iris or fingerprint based quick passage through security at Albany, Cincinnati, DC Dulles, DC Reagan, Denver, Indianapolis, Jacksonville, Little Rock, New York JFK, New York LaGuardia, Newark, Oakland, Orlando, Reno, San Francisco, San Jose and Westchester airports[52].

Canada has a similar system, “CANPASS-Air” that uses iris scanning to allow pre-screened low-risk passenger to clear customs and immigration [33].

In the three scenarios above the iris scans are generally taken indoors and do not expose the iris scanning devices or subjects being scanned to outdoor conditions during the iris image capture operation. This single factor makes them quite different from the conditions anticipated in deployment of iris recognition technology at the gates of port facilities.

4. Warzone Security

Iris scanning has been used in Iraq to screen individuals during Iraqi army recruiting drives. This application is one of the first to move iris scanning technology out of the controlled office environment. The conditions under which registration takes place appear to be inside of tents and building that provide less than ideal conditions. But, due to operational security in Iraq, we were unable to obtain performance data on the program.

Figure 6. Image from Operation Iraqi Freedom shows an Iraqi army recruit being screened against a database to determine if the individual has been detained elsewhere before and to save their identities on file. Photo provided by DOD

5. Other Examples

Prison facilities in Pennsylvania and Florida started using iris recognition in 1999 to facilitate release of prisoners or more appropriately stated to prevent the release of the wrong prisoners [36].

In November, 2002 City Hospital of Bad Reichenhall, Bavaria in Germany installed iris scanners to control access to newborn infants. Here authorized individuals are enrolled and their eyes are scanned prior to gaining access to the infant station [33].

Also in 2002, National Geographic asked Daugman to use his iris recognition algorithms to help confirm the identity of Sharbat Gula. Sharbat had been photographed by Steve McCurry in 1984 at the age of 12 in a Pakistan refugee camp. In 2002 McCurry was able to track Sharbat down and again photographed her [40]. What is most interesting about this application is that neither image was captured using an iris scanner, but rather the determination was made from photographs provided by McCurry. These results were confirmed by Iridian Technologies. [29]

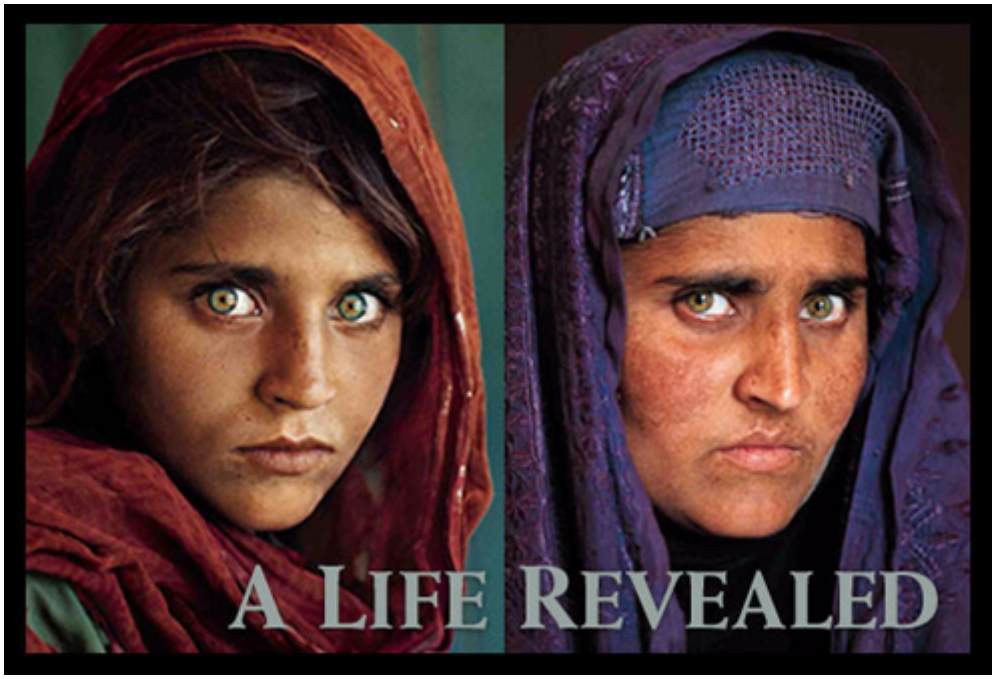


Figure 7. Side by side images of Sharbat Gula an Afghan woman who was originally photographed as a refugee in Pakistan in 1984, and again in 2002. Iris recognition algorithms confirmed it was the same individual after 18 years. © Steve McCurry/Magnum Photos. (From [40])

In 2003 a New Jersey school district installed iris scanners to control access to three particular schools in that district. The system is used to establish the identities of both school employees and parents. The school district uses the system to control who is admitted to buildings after a certain time during the school day and to confirm that parents are authorized to pick up children for early dismissal [33].

Iris scanners are being used to help protect medical records at hospitals in Pennsylvania and Alabama [33]

In 2005 the Hampshire County Sheriff in Massachusetts helped launched the CHILD (Children's Identification and Location Database) project. The system provides a nationally available database to help identify registered individuals [37].

D. CURRENT RESEARCH OR RECENT DEVELOPMENTS

In 2000 a study showed that the irises of identical twins (both identical and monozygotic) showed no stronger correlation between related individuals and unrelated individuals. This established that genetic similarity was not an issue for iris recognition [42].

In 2001 Daugman suggested a potential method to defeat the potential for a replay attack of an iris code sent from a remote source [41].

In 2006 Daugman released results of an examination of the data collected from the UAE expellee program. At the time, the UAE program had collected over 630,000 different iris scans. The iris templates themselves were made available to the University of Cambridge for analysis. The analysis of these templates was used to show that even in large databases of iris templates, the likelihood of a false match is still exceptionally low [39].

IRIS 2006 demonstrated a high degree of interoperability between iris equipment from different manufactures. This research effort used multiple manufactures' iris scanning devices for both registration and recognition. It found that an iris image template registered via one device was able to be matched with a temple generated by a different manufactures iris scanner during recognition operation [58]. This bodes well for the iris recognition industry; interoperability provides the end customer with the freedom to know whatever device they choose to purchase, it will interoperate with iris recognition devices already installed into their infrastructure.

1. Daugman's 2007 Algorithm

In August of 2007, L-1 Identity Solutions announced the release of the Daugman 2007 Algorithm for Highly Accurate Iris Recognition in challenging Environments. L-1 claims that the new algorithm will reduce false rejection rates by as much as a factor of 10. It also claims that this new algorithm will open the doors making iris at a distance and iris in motion possible. These results were obtained from internal testing of the new algorithm [7].

This new algorithm is “designed to overcome image quality issues encountered in more challenging real-world scenarios, such as iris on the move and mobile iris applications. These include off axis or off nadir iris images, occlusions due to eye lashes, non-circular irises and other natural distortions” [7] L-1 also notes the (Iris Challenge Evaluation) ICE 2006 run by NIST, in which the algorithm performed at speeds nearly 50 times faster than it nearest competitor.

The ICE2006 study also suggests that the new “Daugman 2007 algorithm” performed with a lower degree of accuracy than prior results of the original Daugman iris recognition algorithm [38]. If the result were a true representation of the new algorithm’s accuracy it could have seriously impaired the industries desire to deliver devices that could capture iris images for recognition in less than perfect circumstances.

Daugman responded that the ICE2006 results do not give a true representation of the performance of the new algorithm and suggests flaws in the testing methodology [56].

THIS PAGE INTENTIONALLY LEFT BLANK

III. A SURVEY OF BIOMETRIC ATTITUDES

A. SURVEY MOTIVATION

Since the discovery that fingerprints could be used to identify individuals, there have been calls to create a national registry of biometrics for purposes of solving crimes. None of these proposals have ever been implemented due to civil liberties concerns. Following September 11, 2001 there was a tremendous interest in improving levels of security in the Unites States. Biometrics were viewed as being part of the solution to achieving better means of indentifying individuals. The "REAL ID" Act of 2005 requires the standardization of state identification cards including drivers' licenses and other non-driver identification cards. While not requiring states to collect biometrics, the states are not prohibited from collecting them and some states, such as California already do. But REAL ID has met resistance from some groups and some states.

The United States seems to hold to a dual mindset when it comes to identification and the use of biometrics to help achieve it. One the one hand, U.S. citizens seem to desire the Federal government to take action to increase the general level of security by implementing improved methods of screening and identification of those who represent a threat. On the other hand, Americans have also expressed concerns that such information might be misused by the U.S. Government or government officials — for example, as Richard Nixon misused the Internal Revenue Service to harass those on his "enemies" list.

However, most of what we "know", or think we know, about public opinion is anecdotal and based on unscientific media reports and other observations. A review of literature found surprisingly few surveys or other scholarly works that quantified the attitudes of Americans toward the introduction of biometrics into their daily lives.

Technology commentator, Peter de Jager, suggests that any adoption of such technology must consider the beliefs and opinions of the individuals whom will be expected to utilize such technology. He also suggests that no mater how rational or

irrational these beliefs and opinions may appear to those who are in favor of using such technology, or responsible for implementing the use of biometrics; they are still beliefs and cannot be ignored [16]. This would seem particularly true in democracies such as the United States where elected officials have a responsibility to respond to the public's opinion.

With this premise in mind, a survey was conducted concerning attitudes towards the use of biometrics.

B. SURVEY DESCRIPTION AND METHOD

This survey was intended to collect general attitudes concerning the use of biometrics. It presented participants with scenarios of uses of biometric technology by law enforcement agencies, other government agencies and the private sector.

1. General Description of Survey

The first section of the survey was made up of sets of scenarios varying from very limited and specific applications to much more wide-spread applications of biometrics. Much of this sections questions were either based on or taken directly from a 2001/2002 survey conducted by Opinion Corporation [15]. This set of questions provided a set of scenarios that would escalate in perceived levels of infringement on ones "right to privacy" to determination if generalizations could be made about where Americans felt giving ground in privacy was worth the additional security they felt it would bring them. They were also intended to provide a means of comparing our results with those from the surveys conducted in 2001 and 2002 which had 1046 and 1017 respondents respectively.

The second section discussed specific scenarios involving iris recognition. The goal was to assess the respondent's views and knowledge and to try and understand how the choices between privacy and security would be made.

A section followed to inquire about participants concerns with iris scanning and their level of confidence in the ability of iris scanning to differentiate between individuals, and any health concerns about the use of iris scanning.

The Opinion Corporation survey had included a section of questions about participants' experience with both violent crime and identity theft. These questions were added in hopes of seeing a correlation between these experiences and attitudes, in particular, ones willingness to give ground in the area of privacy when compared to those who had not been victims of such crimes.

There was an open-ended request for comments concerning moral or religious objections, or other concerns with the use of biometrics. Also collected was general demographic data about participants. This was used to look at correlations between opinions and demographic groups and to identify possible demographic bias in the group of participants.

The survey is attached as Appendix A.

2. Survey Method

The Biometric Attitudes survey was prepared and distributed via an internet survey website (SurveyMonkey.com). The web based delivery was chosen as it would provide a medium for obtaining a geographically diverse sampling. The survey medium chosen likely introduces a sampling bias. It limits participants to those with internet access and enough computer savvy to navigate to and through the SurveyMonkey web site.

The survey itself was anonymous and no personally identifiable information was collected from participants. However, demographic data was collected.

3. Method of Solicitation

Survey participants were solicited via three methods:

- Adds placed on Craigslist
- Bulletins posted on Social Networking Sites which included Ringo.com, MySpace.com and Facebook.com
- E-mail solicitation of co-workers, family, friends and acquaintances.

We sought approval from the NPS Internal Review Board (IRB) to give away a single Apple iPod Nano as an incentive to encourage participation of individuals through postings to Craigslist.com. This request was denied and we were limited to soliciting respondents without any incentive. This may have limited survey participation to individuals who were personally connected to the author in some way and resulted in further biasing of the survey sample.

C. SURVEY COMPLETION RATE

The survey solicitation resulted in 99 individual survey starts, with 74 respondents completing the survey. This 76% completion rate suggests that some individuals lost interest in the survey or were interrupted while taking the survey. The average time to complete the survey was approximately fourteen minutes.

D. WHO TOOK THE SURVEY

The solicitation methods used for recruitment of respondents made it difficult to identify individual groups among the survey respondents. The solicitation was sent to three distinct groups of potential respondents. The first group were individuals who had a personal connection to the author, the second group were government employees, contractors and military personnel at Fleet Numerical Meteorology and Oceanography Command (FNMOC) and the third being real estate agents and employees at a Monterey, California area real estate firm. Due to the solicitation being sent out to all groups at roughly the same time (within the same day), the use of a single survey URL and the expressed effort to ensure the anonymity of the respondents, it was not possible to distinguish between these groups.

The survey did collect some demographic information from the respondents that provided some insight into potential differences in opinions. These overall results will be presented side by side with the results specific to these groups, with answers that were statistically different being highlighted.

In a future application of this survey it is suggested that a better method of respondent recruitment be utilized, that will ensure respondents from different

advertisements for participation or different social groups, to ensure they can easily be identified. Two suggestions for this would be to use a different URL to collect responses for each group surveyed or to ensure that the groups are surveyed at different times such that their responses are easily identifiable via the dated respondents answered the survey.

1. Political Orientation

Because attitudes of privacy vs. security are often phrased in terms of conservative / liberal politics, we asked respondents to identify their political orientation:

Politically Conservative	Somewhat Conservative	Middle-of-the-Road	Somewhat Liberal	Politically Liberal	Response Count
18	19	18 (26%)	11	4	70
37 (53%)			15 (21%)		

Table 2. Political orientation of respondents.

2. Victims of Identity Theft

Because biometrics have been proposed as a tool for fighting identity theft, we also collected information concerning respondent's personal experience with identity theft. Having been a victim of identity theft turned out to be indicative in a couple of questions of the survey:

Question: Have you ever been the victim of identity theft? Answer Options	Response Percent	Response Count
Yes	19.7%	15
No	71.1%	54
Don't Know	9.2%	7

Table 3. Victims of Identity Theft.

3. Victims of Violent Crime

It was anticipated that the victims of violent crime would be more likely to support the use of biometrics. A small number of respondents (7%) had experienced violent crime: all of which were women.

Question: Have you ever been the victim of a violent crime? Answer Options	Response Percent	Response Count
Yes	6.6%	5
No	90.8%	69
Don't Know	2.6%	2
	answered question	76

Table 4. Victims of violent crime.

This is an area that would have benefited from a much larger survey response. Those who experienced violent crime appeared to be more in favor of the use of biometrics in many scenarios where the overall respondent opinion was less supportive. Due to the small number of respondents identifying themselves as victims, it was difficult to draw statistically sound conclusions.

In future work it is also suggested that more information should be collected from victims of violent crime. It would be helpful to further classify the type of violent crime they experienced, specifically was the crime related to theft, mugging, car jacking – crimes where money was the apparent motivation for the violent crime, as opposed to those who experienced a violent crime where money was not the apparent motivation. This information might further explain the opinions of victims of monetarily motivated violent crimes with regard to the acceptability of certain applications of biometrics.

4. Gender

Gender was suspected to play a role in some of the questions that asked about the use of biometrics to protect children.

Questions: What is your gender? Answer Options	Response Percent	Response Count
Male	54.7%	41
Female	45.3%	34
	answered question	75

Table 5. Gender of respondents.

5. Education Level

Education level was one of several demographic indicators collected by the survey instrument. It ended up helping us identify a potential bias in our survey respondents. According to a March 2007 press release from the U.S. Census Bureau, 28% of Americans had obtained a bachelors degree [43]. This was out of agreement with the demographics collected from survey participants. Of the respondents who answered the question, over 82% had graduated college or a higher level of education.

Some High School	High School Graduate	Some College	Some Technical/Trade Training	Technical or Trade School Graduate
0	0	11	1	1
College Graduate	**Some Post Graduate School**	**Masters Degree**	**PH. D.**	**Response Count**
27	18	14	2	74

Table 6. Education Level of Respondents.

6. Age

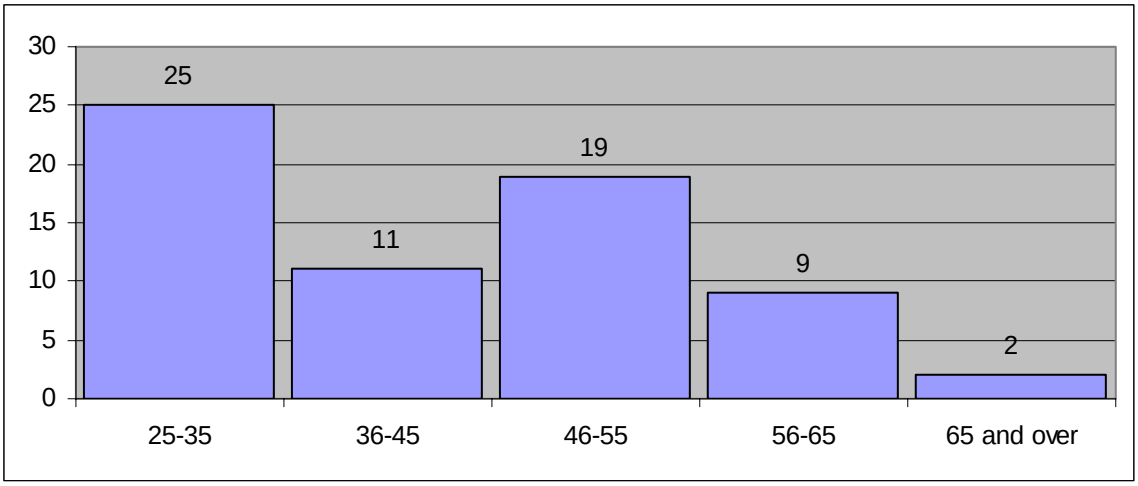


Table 7. Graph of respondent ages.

Survey respondents ranged in age from 25 to 78, with an average age of 43.

E. SURVEY LIMITATIONS

This survey should be considered a pilot study. The largest limitation to the value of the results of this survey is the inability to say much about the respondents and the

relatively low number of individuals who responded to the solicitation for participation. While the responses were not collected randomly, they provided a pool that was sufficient to evaluate the survey itself and provided general insight to public opinion.

This lack of a random survey sampling leads to a potential for future work to repeat the survey, after improvement in some of the questions for clarity and more appropriate options for answers.

F. SEGMENTATION OF RESPONDENTS

We collected demographic data from the survey respondents with the hope of being able to find commonalities between individual respondents and to help understand what some predicative factors might be. We focused on political orientation, gender, and whether or not the respondent had been the victim of identity theft. Finally we separated out the respondents who had been the victim of a violent crime. While there were not enough respondents in this final group (only 5 respondents) to produce any statistically significant analysis, their tendencies to find certain scenarios acceptable was interesting.

G. SURVEY RESULTS

1. Potential Uses of Biometrics by Law Enforcement

We began by asking questions surrounding public safety and the use of biometrics, mostly limited to either identifying criminals or individuals suspected of a crime with a high degree of certainly.

The following questions were asked with this introduction:

> Here are some ways that LAW ENFORCEMENT AGENCIES are using or might use a biometric ID system to identify people. Considering the potential benefits to society, but also keeping in mind the potential threats to privacy, how acceptable would each of these uses be? In your view, would the following scenarios be very acceptable, somewhat acceptable, not very acceptable, or not acceptable at all?

Question 1§: Detectives could take a fingerprint found at a crime scene, turn it into a biometric reading, and use this to search state and federal databases of convicted offenders. (§ 94% acceptable)

§ The 94% acceptable was the result of the 2001 survey conducted by the Opinion Research Corporation on a population 1046. [15]

Results: 100% of respondent found this to be an acceptable use for biometrics.

Table 8. Responses to question 1.

The use of fingerprints to identify suspects at crime scenes is commonplace today and this practice is also presented as normal in many popular television shows. This may contribute to respondents in general being comfortable with this use of fingerprints. In this scenario, an individual would have left a fingerprint at a crime scene in order for their fingerprint to be compared, creating ample reason for them to be subjected to some level of scrutiny.

Question 2§: Police in patrol cars who stopped a driver for highway violations could take a computer scan of a driver's finger, and then use a computer terminal in the patrol car to check this against a database of fugitives involved in serious crimes. (§ 85% acceptable)

Results: Respondents found this to be acceptable as follows:

All (87)	Politically (52)		ID Theft (69)		Male (41)	Female		Victims of (5)
	Conservative	Liberal	Victim	Non-Victim		all(34)	w/o VCV(29)	Violent Crime
80%	76%	87%	80%	83%	78%	85%	86%	80%

Note: Under the category of females w/o VCV means females excluding those who had been Violent Crime Victims. Responses from women who had been violent crime victims are including the "Female- all" column.

Table 9. Responses to question 2.

Here we see a fairly even level of agreement with this potential use of biometrics in the area of law enforcement. One suggestion here is that people find that if an individual has broken a law (the assumption being that if you have been pulled over by a law enforcement officer, you have broken a traffic law) then using biometrics to confirm

your identity is appropriate. It is a common practice today for law enforcement to check for outstanding warrants when they pull an individual over for a routine traffic violation. Again, here the individual would have been either convicted of a crime or highly likely to have committed the crime.

Question 3§: Law enforcement agencies could use finger or hand scan biometrics to allow only authorized officials to enter law enforcement intelligence files. (§ 93% acceptable)

Results: Respondents found this to be acceptable as follows:

All (87)	Politically (52)		ID Theft (69)		Male (41)	Female		Victims of (5)
	Conservative	Liberal	Victim	Non-Victim		all(34)	w/o VCV(29)	Violent Crime
97%	97%	100%	93%	98%	98%	94%	93%	100%

Table 10. Responses to question 3.

Here it appears the respondents felt steps should be taken to protect information held in "intelligence files" and it is appropriate to use biometrics to confirm the identity of individuals seeking access to them. In this scenario, an individual is seeking access to information that is restricted and has the potential to cause public harm if publically released. These responses match very closely to question nine and twelve asked later concerning the protection of "classified" military information.

Question 4§: Police could use facial recognition technology to scan the features of people attending major sports events or public ceremonies, looking for fugitives for serious crimes whose facial formulas they had in their system. (§ 74% acceptable)

Results: Respondents found this to be acceptable as follows:

All (87)	Politically (52)		ID Theft (69)		Male (41)	Female		Victims of (5)
	Conservative	Liberal	Victim	Non-Victim		all(34)	w/o VCV(29)	Violent Crime
64%	68%	80%	73%	67%	**61%***	**76%***	**79%***	60%

* The differences of opinion between men and women here met a 95% confidence level. ($p < 0.05$) with women finding the use of facial recognition in this scenario being more acceptable than men.

Table 11. Responses to question 4.

In this question we asked about the use of facial recognition at sporting events or other public events. This was the least acceptable potential use of biometrics. Here we cross a line where the individual being scanned has done nothing to draw police scrutiny or attention. One possible explanation for the much lower level of support for this application of biometric use might be that individuals believe that by simply attending a public event, they have not broken any laws themselves, and therefore should not be subjected to any form of screening or monitoring. A further issue may be the potential for facial recognition to be done without their knowledge and they may feel this is an invasion of their privacy.

One could argue that individuals do not have to attend the public event if they don't want to be "scanned." After all, no one is forcing them to attend. But when asked about a sporting event, some individuals may feel that sporting events are as American as apple pie, after all baseball is the proverbial "America's pastime." Conducting "monitoring" at such an event might be seen as an overstepping of the authority of police.

For future work, it might be prudent to ask this question twice, with the second question tying the use of facial recognition in this scenario to look for "potential

terrorists" rather than "fugitives of serious crimes." It is possible that under the auspice of protecting the public from a terrorist attack, such scans might be viewed as more acceptable.

The difference of opinion expressed between men and women here might be explained again by the use of "sporting event" in this question. It might be that men tend to place a higher value on their ability to attend a sporting event freely and without any government monitoring of movement, while women may in general feel more vulnerable to being a victim of crime in a public setting.

It is also interesting to note that this was not a political left vs. right question as the differences in responses from the conservatives and liberals are not statically significant.

It is also interesting that this question generated the largest difference between our results and the result from the 2001 and 2002 surveys. In those surveys, 74% of the respondents felt that this was an acceptable use of biometrics. This might be an indication of a shift in public opinion as the memory of the September 11, 2001 attacks have become less fresh on the minds of many Americans than they were in 2001 and 2002; this question was originally asked in late September 2001 by the Opinions Research Corporation[15].

Question 5§: Law enforcement agencies could create a biometric database of all persons convicted of a serious crime, for use in later criminal investigations. (§ 91% acceptable)

Results: Respondents found this to be acceptable as follows:

All (87)	Politically (52)		ID Theft (69)		Male (41)	Female		Victims of (5)
	Conservative	Liberal	Victim	Non-Victim		all(34)	w/o VCV(29)	Violent Crime
98%	97%	100%	100%	96%	98%	97%	97%	100%

Table 12. Responses to question 5.

Here again we may see the acceptance of the respondents to the practice of law enforcement currently building such fingerprint databanks. While today these databanks do not hold everyone's fingerprints, it would seem that individuals are fairly comfortable

with such and idea. In 2001 this question resulted in 68% of respondents answering that this would be a "very acceptable" use of biometrics. Our survey respondents answered it would be "very acceptable" 80% of the time. (When compared to the 2001 survey $p < .05$) This might indicate another shift in public opinion concerning the acceptability of such practices.

2. Potential Uses of Biometrics by Other Government Agencies

The following questions were asked with this introduction:

> Now, here are some ways that OTHER TYPES OF GOVERNMENT AGENCIES might take a biometric reading of individuals and compare it to a stored database of identity formulas. Again, please consider both the potential benefits to society AND also the potential threats to privacy, and then tell me how acceptable each of these uses would be, in your view -- very acceptable, somewhat acceptable, not very acceptable, or not acceptable at all?

Question 6 §: School security guards could screen people entering a school, and compare the scans against a biometric database of convicted child molesters. (§ 88% acceptable)

Results: Respondents found this to be acceptable as follows:

All (84)	Politically (52)		ID Theft (69)		Male (41)	Female		Victims of (5)
	Conservative	Liberal	Victim	Non-Victim		all(34)	w/o VCV(29)	Violent Crime
83%	84%	80%	87%	83%	**73%****	**97%****	**97%****	100%***

* $p < .05$; **$p < .01$; ***$p < .001$ (there were 0 responses of "not acceptable")

Table 13. Responses to question 6.

This question saw statistically significant differences in the answer of self-identified men and women. While only 73% of men found this to be an acceptable use of biometrics, women responded with over 97% finding this to be an acceptable use of biometrics. The most stereotypically obvious interpretation of this would point to the maternal instinct in women. While this may or may not be the true cause, it is apparent that in the group of respondents to this survey, gender appeared to play a strong indicator.

Question 7 §: To prevent people from obtaining double welfare benefits, officials could screen people seeking welfare checks against a biometric database of those eligible for the benefit. (§ 85% acceptable)

Results: Respondents found this to be acceptable as follows:

All (84)	Politically (52)		ID Theft (69)		Male (41)	Female (34)		Victims of (5)
	Conservative	Liberal	Victim	Non-Victim		all(34)	w/o VCV(29)	Violent Crime
89%	89%	87%	93%	91%	**88%***	**97%***	**97%***	100%

* p < .05; **p < .01; ***p < .001

Table 14. Responses to question 7.

Here again we see a gender difference in responses. It might be that women have a stronger sense of "fairness." One other possible explanation could be the placement of this question, as the prior question also elicited a significantly stronger response from women. It is possible that that strong response "bled over", if-you-will to this question and that those who responded strongly to the previous question concerning children continued to respond with great level of support for this application as well.

This result here is somewhat surprising as intuitively it would seem that those who had been victims of identity theft would have been more likely to voice strong support for this application. However, victims of identity theft answer only slight more in favor of this application than the general respondent pool, but not in a way that was statistically significant.

In future applications of this survey it might be beneficial to change the order of the question. Survey Monkey has the option to randomize questions, but we did not use it.

Question 8 §: Election officials could check a biometric database of convicted criminals and others who are not eligible to vote, and bar such persons from voting. (§ 72% acceptable)

Results: Respondents found this to be acceptable as follows:

All (84)	Politically (52)		ID Theft (69)		Male (41)	Female (34)		Victims of (5)
	Conservative	Liberal	Victim	Non-Victim		all(34)	w/o VCV(29)	Violent Crime
80%*	78%	80%	**93%****	**76%****	78%	88%	86%	100%

* p < .05; **p < .01; ***p < .001

Table 15. Responses to question 8.

Identity theft victims seem to be much more supportive of the application of biometrics to ensure voters are who they say they are. It would seem that having experienced the trials that go along with identity theft and the emotion of having someone else pretending to be you might elicit stronger support of methods to prevent such occurrences in voting applications. This was also a significant shift from the 2001 survey results [15] with an increase in acceptance from 2001. This shift might be the result of the political focus on the 2008 Presidential race that was present at the time this survey was administered. In 2001 there was no Presidential race looming in the near future and certainly not the same amount of media attention was being paid to political races.

It is also worth noting that this was not a right vs. left issue with the two groups' responses being nearly equal. This was somewhat counter intuitive as it is often the case that political liberals seem to oppose limits being placed on voters based on strong identity verification or other such limits. This usually seems to be caused by the anticipation that less affluent voters tend toward being liberal voters and that restrictions of this sort are more likely to affect less affluent voters.

Question 9 §: Managers of high-security government facilities, such as laboratories or military bases, could screen people seeking entry against a biometric database of persons authorized to enter. (§ 95% acceptable)

Results: Respondents found this to be acceptable as follows:

All (84)	Politically (52)		ID Theft (69)		Male (41)	Female (34)		Victims of (5)
	Conservative	Liberal	Victim	Non-Victim		all(34)	w/o VCV(29)	Violent Crime
96%	97%	93%	93%	98%	95%	100%	100%	100%

* p < .05; **p < .01; ***p < .001

Table 16. Responses to question 9.

Respondents found using biometrics to protect government research to be acceptable. Here we can theorize that respondents believe that there is not an invasion of privacy involved when an individual seeks access to a government facility such as the one described in the question. This type of facility inherently needs some form of personal accountability of the individuals who seek access, so the addition of biometrics to achieve this is not opposed.

Question 10 §: Immigration officials could sign up persons wanting to speed up entry at passport-control stations, and process travelers more quickly in this way. (§ 85% acceptable)

Results: Respondents found this to be acceptable as follows:

All (84)	Politically (52)		ID Theft (69)		Male (41)	Female (34)		Victims of (5)
	Conservative	Liberal	Victim	Non-Victim		all(34)	w/o VCV(29)	Violent Crime
89%	86%	93%	93%	87%	90%	88%	90%	80%

* p < .05; **p < .01; ***p < .001

Table 17. Responses to question 10.

There is fairly good support for this application of biometrics. One possible explanation is that respondents can envision this application providing some benefit to them. Anyone who has waited to pass through a port-of-entry knows that getting through the passport station can take while, so almost anything to speed along that process might

be viewed positively. The second related explanation is there is currently a high level of concern over border security and respondents may see biometrics as having the potential to help improve border security.

Question 11 §: Government agencies issuing required occupational licenses – such as for teachers, private guards, or nursing home workers – could check applicant's biometric against a database of criminal offenders not eligible to be licensed. (§ 90% acceptable)

Results: Respondents found this to be acceptable as follows:

All (80)	Politically (52)		ID Theft (69)		Male (41)	Female (34)		Victims of (5)
	Conservative	Liberal	Victim	Non-Victim		all(34)	w/o VCV(29)	Violent Crime
89%	86%	87%	87%	89%	85%	91%	90%	100%

* p < .05; **p < .01; ***p < .001

Table 18. Responses to question 11.

Here again, respondents found this to be an acceptable use of biometrics. Privacy does not seem to be a large concern when an individual is given a choice about submitting to a biometric check. When applying for a government issued license there is already some degree of privacy that has been given up through the application process itself. In addition, the very reason for requiring licenses is to protect the public from individuals either unqualified or untrustworthy to conduct certain kinds of business. Thus respondents may see this application as serving the public good, as well as serving their own interests as well.

Question 12: Government agencies could use biometrics to screen individuals who seek access to "secure" rooms that are designed to all the processing of sensitive or classified information, to ensure they have been cleared to have such access

Results: Respondents found this to be acceptable as follows:

All (80)	Politically (52)		ID Theft (69)		Male (41)	Female (34)		Victims of (5)
	Conservative	Liberal	Victim	Non-Victim		all(34)	w/o VCV(29)	Violent Crime
99%	97%	100%	93%	100%	98%	100%	100%	100%

* p < .05; **p < .01; ***p < .001

Table 19. Responses to question 12.

As noted in question three, there seems to be great support for the use of biometrics when protecting "government secrets." This is likely due to the concern over the potential harm that the leakage of classified information might bring about if that information were to fall into the wrong hands. Here the value of protecting the asset in question would seem to outweigh any privacy issue. It is also possible that many of the respondents view this as an application that is not likely to ever directly affect them and therefore there is little concern about the privacy of those who would be subjected to such an application. The contrary also is likely to hold. Those that are likely to be subjected to such devices in their jobs would tend to see this not as an invasion of privacy, but possibly even as an increase in accountability of classified information.

3. Potential Uses of Biometrics in the Private Sector

> Here are some ways that PRIVATE-SECTOR organizations might take a biometric reading of individuals and compare it to a stored database of identity templates. Once more please consider both the potential benefits to society AND the potential threats to privacy, and tell me how acceptable each of these uses would be. In your view, would they be very acceptable, somewhat acceptable, not very acceptable, or not acceptable at all?

Question 13 §: Automated teller machines (ATM's) operated by banks could require a biometric for withdrawing funds in addition to your ATM card and PIN. (§ 78% acceptable)

Question 14: Automated teller machines (ATM's) operated by banks could require a biometric for withdrawing funds without an ATM card.

Question 19 §: Credit card firms could offer card members a biometric to verify their identity for large transactions, and increase the security of credit card transactions. (§ 86% acceptable)

Results: Respondents found this to be acceptable as follows:

Q#	All (78)	Politically (51)		ID Theft (69)		Male (41)	Female (34)		Victims of (5)
		Conservative	Liberal	Victim	Non-Victim		all(34)	w/o VCV(29)	Violent Crime
13	68%	59%	71%	73%	67%	59%	76%	72%	100%
14	60%	57%	57%	67%	61%	54%	68%	66%	80%
19	79%	**76%***	**93%***	**87%***	**78%***	80%	76%	72%	100%

* p < .05; **p < .01; ***p < .001

Table 20. Responses to questions 13, 14 and 19.

We will examine question 13, 14 and 19 together as there are some interesting observations when taken together. While the overall level of support for the application of biometrics for ATM or credit card transactions is not as strong as we have seen for many other government and law enforcement applications, still over 68% of respondents saw protecting their financial assets as an acceptable application of biometric technology. Respondents may be weighting the perceived increase in protection of their own money they would receive, with the potential loss of convenience. It may be that respondents believed that they were likely to experience delays or even the potential for being rejected access to their own money via a false rejection by the biometric device used for verifying their identity.

It is also possible that respondents don't use their ATM and credit cards in the manner they are intended to be used by the banks that issue them. With a card that requires only a PIN number, that card can be "lent" to a trusted family member, who when also provided the PIN, can then access the account on your behalf. If you add the requirement of a biometric verification this changes the arrangement they have with the financial institution. A card with PIN number requires only the token and a secret to be utilized; it does not require the owner to be present! By adding a biometric verification to the mix, that changes, and now the owner no longer has the freedom to allow a trusted party to act on their behalf. This is a loss of convenience, even if it does improve security.

Another potential loss of convenience, which might have been considered by the respondents, is where you are able to use such a card. As this would be the introduction of a new technology to a system that works "adequately" well today, how quick the new readers might be adopted to their favorite shops. If the shops they frequent don't have a reader capable of checking the biometric, they might be denied the ability to shop there.

Victims of identity theft were not significantly more likely to be accepting of this application at ATM's. This might be because identity theft does not happen at ATM's. However, violent crime does happen at ATM's, but it is doubtful that the use of biometrics is likely to reduce that possibility of violent crime, so the lack of difference between these groups may make sense.

However when you up the stakes and ask if they find the use of a biometric check when the transaction is "large" the response of finding it acceptable goes up, from 68% to 79% ($p < .05$). Identity theft victims found this to be more acceptable than their non-identity theft counterparts. This suggests that at some point the risk involved to ones own finances outweigh the potential loss of convenience. An alternative explanation is that a biometric verification is seen as overkill with regular "everyday" smaller transactions, but reasonable when the dollar amount is large "enough." It is also more likely that a retailer that sells items that have "large" price tags would be more likely to install the biometric readers sooner than small item or low dollar shops would be.

Interestingly the political liberals also seemed to find this more acceptable than their conservative counterparts. This result is somewhat counter-intuitive as conservative respondents were almost over three times more likely to have been the victims of identity theft. A free-form question might be a good addition to any future survey; to ask respondents to explain their response to this and other questions.

Question 15 §: Computer system managers could use a biometric to admit persons authorized to access sensitive files, such as medical or financial information. (§ 77% acceptable)

Results: Respondents found this to be acceptable as follows:

All (76)	Politically (51)		ID Theft (67)		Male (39)	Female (34)		Victims of (5)
	Conservative	Liberal	Victim	Non-Victim		all(34)	w/o VCV(29)	Violent Crime
84%	86%	79%	87%	85%	85%	82%	79%	100%

* $p < .05$; **$p < .01$; ***$p < .001$

Table 21. Responses to question 15.

This time we see that when it comes to protecting information that is of some level of confidentiality to the individual (financial or medical records) there is a high level of acceptance of the concept of the added layer of biometric protection.

Question 16 §: Gambling casinos could use facial scanning technology to screen out professional card counters or others banned from gambling in the casinos. (§ 56% acceptable)

Results: Respondents found this to be acceptable as follows:

All (78)	Politically (51)		ID Theft (69)		Male (41)	Female (34)		Victims of (5)
	Conservative	Liberal	Victim	Non-Victim		all(34)	w/o VCV(29)	Violent Crime
56%	**41%****	**79%****	60%	56%	**46%***	**68%***	**72%***	40%

* p < .05; **p < .01; ***p < .001

Table 22. Responses to question 16.

Question 16 is one of the more interesting questions of the survey, and it produced probably the most noticeable divide along political orientation lines. It also resulted in one of the lowest overall votes of acceptability of all the potential uses we suggested. Overall, just 56% of respondents found this to be an acceptable application of biometrics, with conservatives over twice as likely to say they found this to be an unacceptable scenario. Men were also much more likely to find this less acceptable. Women self reported themselves to be slightly more conservative than the men did.

One potential explanation for the lower level of support here could be that casinos are not viewed as a positive societal influence. This might in particular explain the very low conservative acceptance of this application. An alternative theory would be that many individuals feel that casinos are just “legalized thieves” themselves and as such don’t “deserve” to be afforded the level of protection biometrics might provide. It could also be that if facial recognition were used, this could potentially create a record of what “happens-in-Vegas” with the potential for it no longer “stay-in-Vegas.”

Another alternative could be that facial recognition is what the respondents picked up on. This could have been viewed as an intrusive biometric that is acquired by the casino without the individual’s knowledge. This could easily be viewed as an invasion of privacy.

Question 17 §: Employers could check the biometric of job applicants against a government database of convicted felons. (§ 76% acceptable)

Results: Respondents found this to be acceptable as follows:

All (78)	Politically (51)		ID Theft (69)		Male (41)	Female (34)		Victims of (5)
	Conservative	Liberal	Victim	Non-Victim		all(34)	w/o VCV(29)	Violent Crime
82%	**78%***	**93%***	80%	81%	**76%***	**88%***	**86%***	100%

* p < .05; **p < .01; ***p < .001

Table 23. Responses to question 17.

Overall we see a high degree of acceptance of the use of biometrics to check job applicants against a database of felons. It is likely that this is seen as an action that would protect the public from criminals who might otherwise present a threat to unaware individuals. Many jobs require applicants to disclose any criminal history, as a matter of law. The use of biometrics could help to ensure that a deceptive job applicant couldn't simply assume someone else's identity in order to avoid admitting to a potentially disqualifying past.

Here we see difference in the responses between political conservatives vs. liberals; where conservatives were less likely to support this application. It is possible that conservatives felt individuals should be hired on the basis of their qualifications and past job performance rather than any criminal past.

Women were also more likely to see this as an acceptable application than men. This might be explained by women viewing themselves as more vulnerable to a violent crime and as such, found it more important to reduce the risk of working with potentially violent individuals; and there is likely no better indication of violent tendencies than a violent past.

Question 18 §: Stores selling guns could be required to check each person seeking to buy gun against a federal-government database of convicted felons and others not allowed by law to purchase firearms. (§ 91% acceptable)

Results: Respondents found this to be acceptable as follows:

All (78)	Politically (51)		ID Theft (69)		Male (41)	Female (34)		Victims of (5)
	Conservative	Liberal	Victim	Non-Victim		all(34)	w/o VCV(29)	Violent Crime
92%	**89%****	**100%****	100%	91%	**88%***	**97%***	**97%***	100%

* p < .05; **p < .01; ***p < .001

Table 24. Responses to question 18.

When it comes to gun safety there is considerable support for the application of biometrics to ensure only acceptable individuals are able to purchase firearms. In many ways this level of support is not a surprise as it may be seen as an additional step on the part of those who are politically liberal to limit gun sales. To political conservatives it might be viewed as a method to better enforce the current laws surrounding the purchase of firearms, thus possibly reducing the likelihood of new gun control laws. Currently to purchase any firearm in any of the 50 states, an individual must fill out ATF form 4473 which asks the prospective gun purchaser if he or she has ever: a) been convicted of a felony that could have carried a sentence of a year or longer, b) been subject to a restraining order, been dishonorably discharged from the U.S. Military, c) been convicted of domestic violence or having d) been found to satisfy other relevant conditions [46]. An answer in the affirmative to any of those questions prevents the firearms dealer from legally selling a firearm to that individual. However, this form is simply filled out and signed by the customer, and unless the State in which the firearms sale is taking place requires a background check on the sale of all firearms, the dealer can only take the customer at their word. (The "Brady Bill" of 1993 mandates a background check prior to the sale of all handguns only, and not prior to the sale of rifles or other firearms.)

The use of biometrics to confirm an individual's identity and to search registries that would identify an individual as meeting one of the denial criteria would provide the firearms dealer with an additional method to ensure his customer is indeed eligible to purchase a firearm. This would provide a means to enforce the current gun laws more

effectively without requiring more restrictive gun laws to be enacted. Thus gun safety might be increased simply by a more robust application of existing laws.

Conservative respondents were a bit more wary of such an application of biometrics, possible because they might view it as further erosion of their rights under the Second Amendment. Men were also more reluctant to support this application. While there are not direct statistics on the percentage of men vs. women who purchase firearms as not all gun sales are reported to government, it is commonly believed that men are more likely to be gun enthusiasts, so it might be natural for men to be more reluctant to see additional barriers or steps to go through to purchase a firearm.

Question 19: Employers could use biometric scanners to note when employees enter or exit their facilities. For hourly employees, this system would function as a "time-clock." It would also improve employee safety: in the event of a fire or other disaster, the system could be used to immediately produce a list of all employees in a building

Results: Respondents found this to be acceptable as follows:

All (78)	Politically (51)		ID Theft (69)		Male (41)	Female (34)		Victims of (5)
	Conservative	Liberal	Victim	Non-Victim		all(34)	w/o VCV(29)	Violent Crime
63%	57%	71%	73%	56%	61%	62%	62%	60%

* p < .05; **p < .01; ***p < .001

Table 25. Responses to question 19.

In question 19 we present another scenario where individuals have committed no crime or in any way violated any restrictions placed upon them. This scenario received a lower level of support (63%), possibly because it suggests a sort of “big-brother” action by an individual’s employer. However, it would also seem that respondents understood that the employer does indeed have a right to the comings and goings of its employees as employees trade their time for a paycheck.

The scenario also directly suggests that this could improve the safety of all employees and may even imply a certain convenience to respondents with occupations that may require them to “clock-in” each time they begin a shift for their employer and

the idea of being automatically "clocked in" when entering their employers facility rather than after they reach the time clock could be seen as increasing the time they would be paid for.

However, the potential in this sort of scenario for an "automatic biometric time-clock" is the very issue that ILWU members object to so strongly about the TWIC program [61]. In their case, the union representative states that the additional security provided by the TWIC program and any biometric verification of a person's identity does not out-weigh their perception of the program invading their current level of freedom to be at the job site only during the portions of the day when there is work for them to do.

Question 20: Think of a store where you shop on a regular basis. The store has purchased an iris scanner that can scan you as you walk through the front door without the need for you to stop or face in a certain direction. Each time you enter that store your iris will be scanned so that the store can make note of your patronage. The store will use this information to alert employees of your presence (and pull up your recent purchases) so that they can provide you with personalized assistance. If you wish, you will be able to have the system automatically send coupons to your mobile phone as you enter as well.

Results: Respondents found this to be acceptable as follows:

All (78)	Politically (51)		ID Theft (69)		Male (41)	Female (34)		Victims of (5)
	Conservative	Liberal	Victim	Non-Victim		all(34)	w/o VCV(29)	Violent Crime
21%	16%	36%	20%	20%	15%	29%	28%	40%

* p < .05; **p < .01; ***p < .001

Table 26. Responses to question 20.

This scenario was probably the most invasive suggested use of biometrics and not surprisingly received the lowest level of acceptability from survey respondents. This low level of acceptability (over 76% of respondents found this to be somewhat or very unacceptable) strongly suggest that individuals are not comfortable with any method of identification or individualized monitoring in situations that today do not require it. Furthermore, there is no suggestion of this application improving the safety of patrons and even the added benefit of having individually select coupons sent to the patron does not seem to outweigh the perceived invasion of privacy.

Interestingly, this may be an issue of when the store is able to identify the patron. Today, stores are able to track the purchases of their customers whenever a customer pays using a credit card or debit card. Many stores offer "reward programs" that incentivize their customer to allow the store to track their purchases even when paying with cash. So the real issue may be that in this scenario, patrons are made uncomfortably aware of the insight the store may have into their habits.

4. Possible Scenarios for Iris Recognition

In the next section, we shift our focus to iris scanning in particular and away from biometrics in general.

Questions 21-26: When asked if they agreed with the following statements. Respondents answered as follows:

	All	Politically		ID Theft		Male	Female		Victims of
		Conservative	Liberal	Victim	Non-Victim		all	w/o VCV	Violent Crime
I would be comfortable having my iris scanned **to obtain a credit card.**	**33%**	27%	36%	47%	28%	24%	44%	41%	60%
I would be comfortable having my iris scanned **to obtain a passport.**	**63%****	62%	57%	67%	61%	61%	68%	66%	80%
I would be comfortable having my iris scanned **to obtain a driver's license.**	**47%***	41%	57%	40%	46%	46%	50%	45%	80%
I would be comfortable having my iris scanned **to obtain a social security number.**	**59%****	46%	64%	60%	54%	54%	68%	66%	80%
I would be comfortable if **hospitals gave newborns iris scans.**	30%	22%	36%	33%	28%	**20%***	**44%***	41%	60%
If the U.S. Government were to collect iris scan of everyone in the United States, I believe that the iris scan would only be used for official purposes such as confirming a person's identity at an airport.	**22%***	19%	21%	33%	20%	15%	32%	31%	40%

* p < .05; **p < .01; ***p < .001 (Statistical significance when compared to question 21 – to obtain a credit card.)

Table 27. Responses to questions 21 – 26, potential uses of iris recognition. Percentages indicate those that agreed with the statement. The box indicates a statistically-significant difference between men and women.

Respondents indicated that they were more comfortable than not in two of the proposed scenarios: obtaining a passport and obtaining a Social Security Number, 63% and (59%). Respondents were more comfortable with providing an iris scan when it came to security or in dealings with the Federal Government. Only one-third of respondents indicated they would be comfortable with providing an iris scan to obtain a credit card and slightly less than half of the respondents were comfortable with providing an iris scan to obtain a drivers license.

Women were twice as likely as men to be comfortable with allowing hospitals to collect iris scan of newborns; however, this was still less than half of all women. Again this is likely due to the maternal instinct.

The level of mistrust of the government was somewhat inconsistent with overall results in this group of questions. The only two scenarios that more than half of the respondents found acceptable were both scenarios that required dealing with the government, while less than one in four individuals stated they trust the government not to misuse that information. There are two possible explanations that stood out: One is that these same individuals trust the private enterprises they would be dealing with in the other two scenarios even less than they trust the government. However, the more likely explanation for this apparent disconnect is that the governmental interactions suggested are the basis for establishing an individual identity in almost every facet of live in America.

5. Mistrust of Government

The best explanation of the low levels of support for such scenarios might be indicated by the last question in this section. Less than one-quarter of the respondents believed that the U.S. Government could be trusted to use iris scans for "official purposes." This suggests that individuals feel that any such collection of biometrics and iris scans in particular would inevitably be used for purposes that might be either considered "unofficial" or go beyond the uses the U.S. Government was authorized to use them for. The survey allowed respondents to give a free response to this question — some of the responses are illustrative.:

- "No, however, my approval of biometrics corresponds exactly to the level of trust for my government. As such, if I were Chinese or Russian, my answers would be very much opposed."
- "No. But I do oppose the collection and storing of this type of information from innocent people, in light of what the government would do with it once it has been collected."
- "Not really--I tend to view it as inevitable. Human nature being what it is/prophecies having been made 1000's of years ago, I know they will eventually be greatly misused."
- "I believe that we all have right to privacy and that biometrics will eventually be used to track our individual activities well beyond what we comfortable today. Eventually, I think [biometrics] will facilitate the acceptance of the Biblical "Mark of the Beast." But that is more about where biometric use could and probably will lead rather than the use of biometrics themselves."

These responses indicate that some respondents simply feel it is an unavoidable and foregone conclusion that if given the ability to identify its citizens without their knowledge (both iris and facial recognition present this potential), that the U.S. government will eventually misuse this ability. Two of the above responses also indicate a perceived tie between biometrics and the "Mark of the Beast" discussed in Revelation 13:16-18.

6. Confidence in Iris Recognition Technology

Questions 27-29: When asked their opinions of the effectiveness and trustworthiness of iris recognition respondents agreed with the following statements as indicated.

	All(76)	Politically (51)		ID Theft (69)		Male (41)	Female (34)		Victims of (5)
		Conservative	Liberal	Victim	Non-Victim		all	w/o VCV	Violent Crime
I think that iris scans are **unique for each individual.**	67%	65%	50%	73%	65%	71%	62%	55%	100%
I think that the patterns on an **iris can be duplicated well enough to fool a scanner.**	20%	**24%***	**7%***	0%	24%	22%	18%	17%	20%
I think that it will become so easy to duplicate an iris that, **if iris scanners were widely used, iris prints would be stolen on a regular basis.**	20%	**30%***	**7%***	27%	31%	22%	18%	21%	0%

* p < .05; **p < .01; ***p < .001

Table 28. Respondent opinions concerning the trustworthiness of iris recognition.

Over half of the respondents answering (40 out of 76) did not know if irises could be duplicated; this indicates unfamiliarity with the technology. No victim of identity theft believed that it was not possible to duplicate an iris well enough to at least fool an iris scanner, and political conservatives were more trusting of the technology than were liberals.

Again, one of the responses to having any moral or religious objections sums up one of the potential problems if biometrics sources are replicable;

- My concern is the storage and theft of biometric data. Biometric data theft could make clearing ID theft harder...If your fingerprint/iris scan was used fraudulently...you cannot just get a new one. I feel databases of known criminals used to identify criminals in specific situations where it is illegal to participate is fine but random public scanning would not be OK.

7. Fear of Injury for Iris Scanners

Questions 30-31: When asked if they had any concerns of physical injury from iris scanners, respondents said they did have some concern of injury as follows:

Question 30: Do you have any concerns of physical injury with the use of iris scanners

All(76)	Politically (51)		ID Theft (69)		Male (41)	Female (34)		Victims of (5)
	Conservative	Liberal	Victim	Non-Victim		all	w/o VCV	Violent Crime
35%	39%	50%	20%	40%	33%	36%	34%	35%

After providing the following explanation: An iris scanner works by taking a picture of your iris and then compares that image to a known sample of your iris. In most cases, the photo taken poses no more risk that a regular picture taken by any camera. The respondent were then asked:

Question 31: Knowing this, do you now have any concerns of physical injury?

All(76)	Politically (51)		ID Theft (69)		Male (41)	Female (34)		Victims of (5)
	Conservative	Liberal	Victim	Non-Victim		all	w/o VCV	Violent Crime
28%	33%	36%	13%	32%	25%	29%	24%	28%

Table 29. Respondents who had a fear of physical injury from iris scanning

Here we see that respondents did in fact believe that there was risk of physical injury from an iris scanner. After being given a short explanation of how an iris scanner works, the level of fear seemed to diminish.

However, the wording of the question left some real ambiguity as to how the respondent should answer. The question asked respondents to choose from the following possible answers: “Strongly Disagree”, “Somewhat Disagree” “Neither Agree or Disagree” “Somewhat Agree” or “Strongly Agree.” This left the respondent to not only gauge their level of concern but then to decipher if agreeing meant they had some concern or had no concerns. If this survey were to be re-administered, the wording of this pair of questions should be corrected to ensure respondent choices are clear.

8. Awareness of Identity Theft Methods

Respondents were asked: "Some individuals fraudulently assume the identity of other persons in order to engage in illegal acts. To the best of your recollection, have you ever read or heard about people doing this in any of the following ways?"

Question 32 §: Respondents answering (77)	Yes	2001
To apply for government welfare payments to which they were not entitled	77%	50%
To cash forged personal checks	83%	62%
To use stolen credit cards	89%	72%
To obtain a credit card in someone else's name	86%	62%
To obtain unauthorized access to confidential computer files	66%	52%

Table 30. Responses to question 32, concerning awareness of identity theft compared to responses from the 2001 survey.

This question only confirmed that individuals have indeed heard of identity theft and we see an increase in familiarity from the 2001 survey conducted by ORC. This could be due to increased media attention identity theft has received in recent years.

Question 33 §: How serious a problem do you think this sort of thing poses today?					
77 Respondents answering	Very Serious	Somewhat Serious	Not Very Serious	Not Serious at All	Don't Know
I would say this problem is :	61	15	1	0	0

Table 31. Responses to question 33.

Nearly all respondents felt that identity theft was a serious problem. This was in line with the 2001 responses as well.

9. Protection or Criminal Treatment

The survey asked how respondents felt about the use of fingerprinting and iris scanning. Did they feel these techniques treated the individual as a criminal or helped to protect individuals and the public from fraud?

Method of Biometric Respondent answering (75)	Treats like a presumed Criminal	Protects against fraud	Don't know
Question 38: Fingerprinting	81%	7%	12%
Question 40: Iris Scanning	64%	8%	28%

Table 32. Respondent answers to questions 38 and 40.

These two questions reveal a difference in the ability of respondents to form an opinion concerning iris scanning, as over one-quarter of the respondent's did not know or were unable to decide if the method treated individuals like presumed criminals more than it protected against fraud. This could be due to the lack of familiarity with iris scanning as a practice or technology, but it might also be due to respondents feeling that it did both and were unable to pick one answer being the stronger impression or possibly that they could not choose one response over the other.

If this question was used in a future survey, it might be prudent to offer a fourth option of "Both." This would help to determine if individuals really did know or if they were torn between the two options.

H. SURVEY RESULT SUMMARY

One of the trends that seemed to be persistent throughout the survey results was that respondents were generally open to the idea of using biometrics to enhance the ability to establish or confirm the identity of individuals in situations where there was already a requirement to establish the identity of an individual. It seemed possible to sway their opinion on certain situations if there was some sort of law enforcement angle added to the scenario (think of the sporting event question.)

There was a much less of an open-minded attitude when either the application of biometrics would establish identity in new situations, or in particular, where biometric identification was being done without their knowledge. The sporting event received the lowest level of support of the initial law enforcement scenarios. In the potential

commercial scenarios, when it was suggested that a store could use such technology to identify customers when they entered the store, the level of support was even lower.

1. TWIC Implications

Question 19 asked about an employer using biometrics to act as an "automated time-clock." Here we see a much lower level of support for such an idea than for other law enforcement and governmental applications of the biometric technologies.

This result is probably the most significant result from the survey itself with regard to the TWIC program. With a much larger sample set it would be prudent to add a question to ask the respondent if they worked at a job where they currently clock-in and out, or if they work in more of a salary or till the job is done occupation. This might show even further opposition to this concept among the later group.

Question 26 also indicated an overall mistrust of the U.S. Government to expand the use of any collection of biometric data beyond the original intended use. This particular opinion is very strongly held by the ILWU and will need to be addressed if there is any hope of the ILWU acting in a supportive manner toward the TWIC program.

I. FUTURE WORK

In the end, the largest limitations to the value of the results of this survey ended up being an inability to say much about the respondents themselves and the relative low number of individuals who responded to the solicitation for participation. While the subjects were not randomly selected from the general population, they provided a pool that was sufficient to evaluate the survey itself and provided general insight to public opinion.

This lack of a random survey sampling leads to a potential for future work to repeat the survey, after improvement in some of the questions for clarity and more appropriate options for answers as indicated in section III.I.1. If repeated, it is recommended that a more formal method be used to acquire a more random sampling, or that a more targeted audience be sought in order to be able to say something valuable

about that particular audience. One such audience would be members of the International Longshore and Warehouse Union (ILWU), who will be directly effected by the TWIC program and its future implementation of biometrics as a means of identity verification.

Throughout the results section there are suggestions for improvements to the questions that were asked and suggestions for additional questions that might help to further clarify some of the underlying indicative commonalities among individuals who were resistant to certain applications of biometrics.

1. Suggestions for Improvement of this Survey

Below are some suggested ways to improve this survey.

a. Identification of Respondent Groups

In a future application of this survey it is suggested that a better method of respondent recruitment be utilized that will ensure respondents from different advertisements for participation and/or different social groups can easily be identified. Two suggestions for this would be to use a different URL to collect responses for each group surveyed or to ensure that the groups are surveyed at different times such that their responses are easily identifiable, via the dated responses to survey.

b. Further Classification of Victims of Violent Crime

In future work it is also suggested that more information be collected from victims of violent crime. It would be helpful to further classify the type of violent crime they experienced, specifically was the crime related to theft, mugging, car jacking – crimes where money was the apparent motivation for the violent crime, as opposed to those who experienced a violent crime where money was not the apparent motivation. This might further separate victims of violent monetary motivated crimes and their opinions of acceptability toward certain applications of biometrics.

c. Restatement of Purposes for Facial Recognition at a Sporting Event

For future work, it might be prudent to ask this question four (4) in two different ways, with the second question tying the use of facial recognition in this scenario to look for "potential terrorists" rather than "fugitives of serious crimes." It is possible that under the auspice of protecting the public from a terrorist attack, this might be viewed as more acceptable.

d. Additional Demographic Questions

It might be possible to shed further light on apparent gender differences seen in question six (6) by adding a few demographic questions to this survey, to include asking if the respondent had children and the ages of those children. This might shed some insight as this could instead be a parental issue rather than a gender issue.

e. Improve the Iris Education Effects on Safety Concerns

Two questions were asked about the level of concern over physical harm due to iris scanning. If this survey were to be re-administered, the wording of potential answers to these questions should be reworded to make the selection more appropriate to the questions. The questions asked:

Do you have any concerns of physical injury with the use of iris scanners? Respondents were provided with potential answers ranging from strongly agree to strongly disagree. Answers presenting a range of "great concern" to "no concern at all," would be much clearer.

g. Criminal Treatment or Fraud Protection

The survey asked how respondents felt about the use of fingerprinting and iris scanning. Did they feel these techniques treated the individual as a criminal or helped to protect individuals and the public from fraud or didn't know? If this question was use in a future survey, it might be prudent to offer a fourth option of "Both." This would help to determine if individuals really did know or if they were torn between the two options.

h. Free Form Response to Explain Question 19

Question 19 concerning the acceptability of using biometrics to protect large transactions made with credit cards produced a somewhat counter intuitive divide along lines of political affiliation. It would be useful to add a freeform question to ask respondents to explain their reasoning.

i. Add Comparative Rating Question

It would also be interesting to add a question that specifically asks respondents if they would be more comfortable using iris recognition or fingerprint scanners if they are required to provide a biometric for identification purposes. This might provide the ability to make additional recommendations to policy makers of individual government programs if the survey was administered to groups who would be required to comply with those individual programs.

IV. TEST OF PIER 2.3 IRIS SCANNER

A. EXPERIMENT MOTIVATION

This experiment was intended to test the reliability of a handheld iris scanner in field conditions. While iris scanning is used in various scenarios around the world, they are typically deployed in office-like environments where the environmental conditions are fairly stable and there is an expectation of cleanliness. A search of the literature found little data on the reliability of iris scanners in less than ideal conditions and operated by personnel who had received minimal training. The eventual target of using iris scanners in the port environment would present conditions that could be far from ideal. Compared with other biometrics, such as fingerprints or facial recognition; iris scanning would seem to have an advantage in these environments: even when a person's hands are covered with gloves and the face is bundled up, the eyes (and the irises) are still visible.

Most of the scientific evaluations of iris scanning utilize large iris template databases and a large number of iris templates collect via an iris scanner prior to the experiment itself. The collected iris templates are then compared to the template database. These experiments are often focused on the speed at which a particular algorithm can process large volumes of collected templates and the accuracy of the matches when presented with clean data.

Iris scanners have been deployed to war zones in recent years [59] and have been used in conditions that are less that ideal, but there is little public information about the reliability of these devices in those scenarios.

With the scenario of an iris scanner being used to confirm the identity of individuals seeking access to a facility, and the scanning to take place while these individuals were still in their vehicle, we set out to design an experiment that could test the reliability of a hand held iris scanner in such an environment.

This experiment utilized volunteers, both for the participants being scanned, as well as the individuals who operated the device. This allowed us to assess the device from a somewhat technical standpoint of reliability as well as its ease of use.

B. EXPERIMENT SET UP

1. General Description of Experiment

For this experiment we used a Portable Iris Enrollment and Recognition (PIER) 2.3 handheld unit. Volunteers were identified and registered using the PIER 2.3. The PIER 2.3 operators were also volunteers who had some experience standing watch in military settings. The week following registration the experiment was conducted. During the experiment, participants would drive onto the facility we used and, after receiving official permission to enter the facility, the participant would stop their vehicle near the scanner operator. The scanner operator would then greet the participant and ask if it was okay to scan their iris. If given the go ahead, the operator would the attempt to scan the iris of the driver.

2. Why this Location

The FNMOC campus houses a workforce of approximately 600 personnel. The physical layout of the ground allowed for volunteers to participate in the iris scanning experiment without leaving their vehicles while at the same time creating a low likelihood of blocking other automotive traffic seeking entry; thus presenting less disruption to normal facility operation.

Fleet Numerical Meteorology and Oceanography Center (FNMOC) was chosen for three primary reasons:

The physical location of FNMOC. FNMOC is located in Monterey California and sits just over 1 mile from the shore line of Monterey Bay. This location appeared to be ideal as it would likely provide weather conditions similar to those present at the gate of a typical port facility. This was desirable for duplicating the target condition for conducting a field experiment of how reliably an iris scanner would function in

environmental conditions present at a port facility. As mentioned in chapter one, the AAPA had voiced strong concern to the implantation of the TWIC program due to a lack of testing of biometric readers and TWIC card readers in the port environment [4]. It was hoped that the choice of FNMOC would provide a field experiment that met at least some of this particular concern. As FNMOC is a gated facility, the iris scanner could be used on volunteers as they entered the facility and while they were still inside of their vehicle.

Figure 8. Map of the location of Fleet Numerical Meteorology and Oceanography Center (From Yahoo Maps)

FNMOC is a fenced and guarded facility. Individuals who seek entry to the FNMOC facility are required to stop at a guard shack and present identification to an armed guard prior to being allowed access to the facility. This provided a pool of potential volunteers who were accustomed to being stopped prior to gaining access to a

gated facility. We thought this pool of volunteers would be less likely than the general public to see the requirement to take an extra 20-30 seconds upon each entry to the facility as an unacceptable inconvenience. FNMOC also presented an opportunity to have a pool of volunteers who would not need to go out their way to participate in this experiment. Volunteers worked at this facility, and thus they would drive through the gate of the facility as part of their regular routine and participation in the field experiment would therefore require very little deviation from that routine.

The experiment itself took place over one week; participants had their irises scanned each time they entered the facility during that week. There was concern that potential volunteers might not be willing to take the time required for briefing, IRB consent or debriefing even though the experiment itself had a minimal time requirement.

The author had served a previous tour at FNMOC and had many friends and acquaintances that work at this facility. These personal contacts were important to the success of the experiment as we were limited in the amount of compensation we could provide to volunteers.

3. Participants

All volunteers were either members of the U.S. Navy, DoD civilian employees or DoD civilian contractors who were stationed or worked at Fleet Numerical Meteorology and Oceanography Center (FNMOC) in Monterey, California. The scanner operators were also volunteers and were all active duty member of the U.S. Navy stationed at FNMOC.

a. Biographic Breakdown

There were a total of 25 volunteers who agreed to register their irises both left and right with the PIER 2.3 unit. All biographic data was self reported by the participants.

b. Gender

Gender		
Male	21	84%
Female	4	16%

Table 33. Experiment Participant Gender

c Eye Color

Eye Color		
Blue	10	40%
Blue-Green	1	4%
Brown	7	28%
Dark Brown	1	4%
Hazel	6	24%

Table 34. Experiment Participant Eye Color

d. Age Groups

Age Groups		
20 – 29	8	32%
30 - 39	4	16%
40 - 49	6	24%
50 - 59	6	24%
60+	1	4%

Table 35. Experiment Participant Age Groups

e. Wears Corrective Lenses

Corrective Lenses		
Eye Glasses	7	28%
Soft Contacts	3	12%
Hard Contacts	1	4%
Both	2	8%
None	12	48%

Table 36. Experiment Participants Corrective Lenses

4. How Participants Were Recruited

Participants were sent an e-mail solicitation that had been approved by both the NPS IRB and the Executive Officer of FNMOC, sent from the Executive to all hands at FNMOC. (See appendix B.) This initial e-mail was intended to draw interested personnel to a presentation where they could learn about the experiment and what would be required of them. This presentation was given on 29 Nov 2007 at FNMOC by the author to approximately 15 personnel who attended. (Presentation is Appendix C.) During this presentation, potential volunteers were provided a brief history of the laws that had been passed (the ATSA and the MTSA) to bring about the TWIC program and how iris scanning might impact the deployment of the TWIC program.

People who wished to volunteer were asked to sign up for a time slot later that day to return and have their irises registered into the system. The experiment received 25 volunteers in all.

5. Why the PIER 2.3

While looking at options for iris scanners to use for this experiment, one of the most important requirements was that the device had to be mobile and allow for quick set up and tear down of the unit as the experiment would take place during limited blocks of

time during the day. (This will be explained further in section IV.C – Experiment Method.) There was also a desire to test a unit that would allow for maximum repositioning to fit the location of the driver both in reference to the device itself as well as the subject location within the vehicle.

We also wanted to allow for the scanning irises of volunteers walking to work. This later scenario of a walking individual having their iris scanned was not initially part of the scope of the experiment, but some of the volunteers routinely walk to and from the FNMOC gated facility, in particular for lunch periods, so we needed to accommodate this scenario. During visits to the Port of Oakland to see the actual conditions that an iris scanner would need to accommodate, we learned that at some facilities many of the longshoremen, who work exclusively on the waterfront, park outside of the port facility itself and then gain access to the port via a turnstile. Thus testing a subject on foot turned out to be a very appropriate scenario.

The PIER 2.3 was chosen as it was a handheld iris scanning unit, its use in operational environments such as Iraq and it was identified as a having the best recognition image quality distribution of the units tested in the IRIS06 Iris recognition Study[44].

The PIER 2.3 can be operated in a non-tethered configuration and this was seen as a positive for the purpose of this experiment. This would allow for an individual to operate the system as opposed to a fixed unmanned unit, who could then record conditions or observations if and when the unit failed to recognize a participant.

The Pier 2.3 is also a ruggedized unit that would withstand minor rough handling that might be experienced during the normal operation of the device while using it to collect iris scans of individuals who were seated inside of a vehicle during the scanning process. The PIER 2.3 weighs just over a pound (16.5 oz) and can be used in the field with battery power and with no other cords attached. This was anticipated to be advantageous as we did not how much flexibility in positioning the operator might need to get recognizable scans while the subject was sitting in a vehicle.

SecuriMetrics, the manufacture, was also kind enough to lend us a PIER 2.3 for the duration of the experiment. This reduced the costs associated with the experiment and provided some additional flexibility for other un-anticipated expenses that might be encountered later on during the course of the experiment, survey or thesis research.

C. EXPERIMENT METHOD

1. How Participants Were Registered

Step one of using any biometric system is to register users into the system. For this experiment we registered volunteers at FNMOC later in the day after the informational brief about the experiment was given. Registration of volunteers including the following steps:

Volunteers were registered the week before the experiment. Training of the operators took place that same day with the exception of a single operator who was absent that day. That absent operator was trained on the following Monday by one of the other operators. The field experiment of the PIER 2.3 took place the following week. There was very little time between registration and the field experiment itself.

Volunteers read and signed a Privacy Act and Informed Consent form informing them of their rights and the experiment conductor's responsibilities to the volunteer.

Volunteers then filled out a Biographic Questionnaire to provide:

- Eye Color
- Gender
- Age
- If they wore corrective lenses, their prescription if they where willing to share it and/or knew it – most even if willing to share that information did not know it.
- Any Eye conditions the subject currently or previously had experienced. Lasik surgery was the condition reported most often by those who reported a condition.

Volunteers were then provided an informational sheet that provided instruction on what would be expected of them to participate in the experiment and a reminder that they could excuses themselves from the experiment at any time.

Attached to this informational sheet were two small green stickers with the volunteer's subject number. One of these stickers was to be placed on the windshield of their vehicle just above their DoD sticker to identify themselves to the scanner operator as a participant.

Figure 9. An example of the green sticker that was placed above the DoD stick on the volunteers' vehicle to identify themselves as participants to the scanner operator. To excuse oneself from the experiment this stickers was simply removed. (image: Simon McLaren)

Both their left and right irises were then scanned and registered in the PIER 2.3 unit used for the experiment. Subjects were registered in the system as Last name: SUBJECT, First name: J.

Figure 10. Image of a registered iris after recognition. All subjects for this experiment were named J. Subject and differentiated only by the Eye R ID and Eye L ID numbers. (image: Simon McLaren)

The registration of volunteer's irises took place in a typical office-like environment where light conditions were similar to what one would expect in such and environment. This would not be the conditions that would likely be experienced at the gate when the volunteers would eventually be scanned to test the device, allowing a possible error in the experiment.

This discrepancy between the registration conditions and the conditions at the time of the testing were allowed as this was a field test of the device. This was also expected to resemble the real world if the iris scanning device were to be deployed at a gated facility where scanning takes place outdoors. In this scenario, it would be most likely that the initial registration of the irises of a subject would take place in the comfort of an office, where the individual conducting the registration was likely to be located.

It would be impossible to register and individual in conditions that would be experienced at the time of recognition in a real world deployment as lighting conditions vary greatly during the day due to the position of the sun as well as due to the changes in weather conditions that will be experienced. Thus the registration of the irises in office like condition was deemed to a very life-like scenario.

2. The Spoiler

One volunteer was chosen at random to not be registered in the PIER 2.3. This volunteer placed the green sticker on their vehicle just like all the other volunteers. This volunteer agreed to have their iris scanned each day during the experiment to allow for an opportunity for a false accept within the limits of our small sample set. This was to simulate a scenario where someone who was not authorized to access the port was seeking access. The question here was, "would the PIER 2.3 correctly fail to recognize this individual?"

In the case of securing a facility via iris scanning, this would most likely represent the largest threat to the facility. Those whom are registered in the system might also represent a threat, but in this case, the device should be expected to correctly recognize that individual and it would be up to the information stored in the registration database to then notify the operator that the individual was deemed a threat or to automatically deny the individual access to the facility or whatever asset the scanner was intended to protect.

3. Scanner Operator Training

In addition to volunteers that would allow their irises to be scanned we also recruited volunteers to operate the PIER 2.3 iris scanner during the week of the experiment. Utilizing volunteers to operate the device allowed an opportunity to evaluate the ease of use and ease of training of the device.

The thesis author was trained by Tim Johnson, Senior Sales Consultant for SecuriMetrics at their Martinez, CA office location. Mr. Johnson provided a hands-on training session with the PIER 2.3 device, as well as a familiarization with the HIIDE series 4 (Hand-Held Interagency Identity Detection Equipment) device during the

training session. SecuriMetrics also provided a DVD training video that included additional training on the use of the PIER 2.3.

The four volunteer PIER Operators were trained the week prior to the field study via the SecuriMetrics Training DVD the day of the informational presentation and allowed a period of hands-on familiarization with the device. One of the four operators was not present the day of training and the author decided to allow one of the three operators who had been previously trained to provide the familiarization training to the fourth operator without the benefit of the DVD.

4. The Actual Experiment

During the week of the experiment, Dec 3 - Dec 7, 2007, the PIER operators took positions at the entrance to the FNMOC facility. Scanning subjects were instructed to drive onto the facility and, after receiving official permission to enter, the subject would stop their vehicle near the scanner operator. The scanner operator would then greet the subject and ask if it was okay to scan their iris. If permission was given, the operator would proceed to position the scanner the recommended 4" to 6" from the subject's eye and attempt to collect a scan of their iris.

- If the scan was successful the operator checked to see if the subject number displayed by the scanner matched the subject ID number on the subject's placard. The operator also recorded whether the subject was wearing glasses or contacts and estimated the amount of time that it took to scan and identify the subject.
- If the scanner failed to recognize the subject, the operator would record the same information and complete a short form recording any observations they noted that might have contributed to the failure to recognize. The operator would then try the scan again, and again would record the same information. The operators were told not to attempt to recognize a subject any more than three times on a single attempt to enter the facility.

If a subject entered on foot, the procedure was the same with the exception of the subject standing still in front of the operator instead of sitting inside a car. The operator recorded the same information about the attempt and success or failure.

5. Time Frame of the Experiment

Scans were performed from 0730–0930 and from 1130-1330 on each day of the experiment, these times being chosen to match the morning commute and lunch hours of FNMOC. This allowed for the possibility of scanning each subject at least twice each day, and increased the likelihood of being able to scan those subjects that usually arrived prior to 0730 in the morning on their return from lunch.

These time frames led to one shortcoming of the experiment: it would have been informative to have included time outside of those time windows, as these windows did not provide an opportunity to test the device in low light or nighttime conditions. Both of these light conditions are likely in any real world deployment of iris scanners to confirm or establish the identity of an individual seeking access to a gated facility. These times are sure to be part of the routine at a port facility.

6. Eyeglasses

We tested subjects both with and without glasses. Given the scenario of utilizing an iris scanner at a gated facility while drivers are still inside their vehicle, it is reasonable to assume that some drivers will be wearing eye glasses and would forget to remove them on occasion even if trained to do so.

Subjects who wore glasses were instructed to remove them or lift them over the eyebrows to be scanned on day one and two. Day three through five subjects who wore glasses were instructed to leave them on as the experiment attempted to determine how eye glasses affected the reliability of the device.

D. OBSERVED RESULTS

1. Observed Failure Rates

a. Failure to Register

We did not experience any failures to register with any of the 24 volunteers whom we attempted to register in the device. However, we did experience a difficult time registering two of the subjects. Both required multiple attempts to acquire acceptable images from at least one eye during registration.

An acceptable image for registration is one that is at least 90% in focus as indicated by the focus bars on the PIER 2.3 device. Below are two images that show an attempted recognition scan and two level of focus. There are two focus indicators on the PIER 2.3 screen. There is a green indicator bar on the left and one on the right of the iris image. The left bar is used to indicate focus levels of 0-90% and the right bar indicates focus level of 90-100%. An acceptable image is one that is at least 90%. The second image shows an acceptable iris scan image.

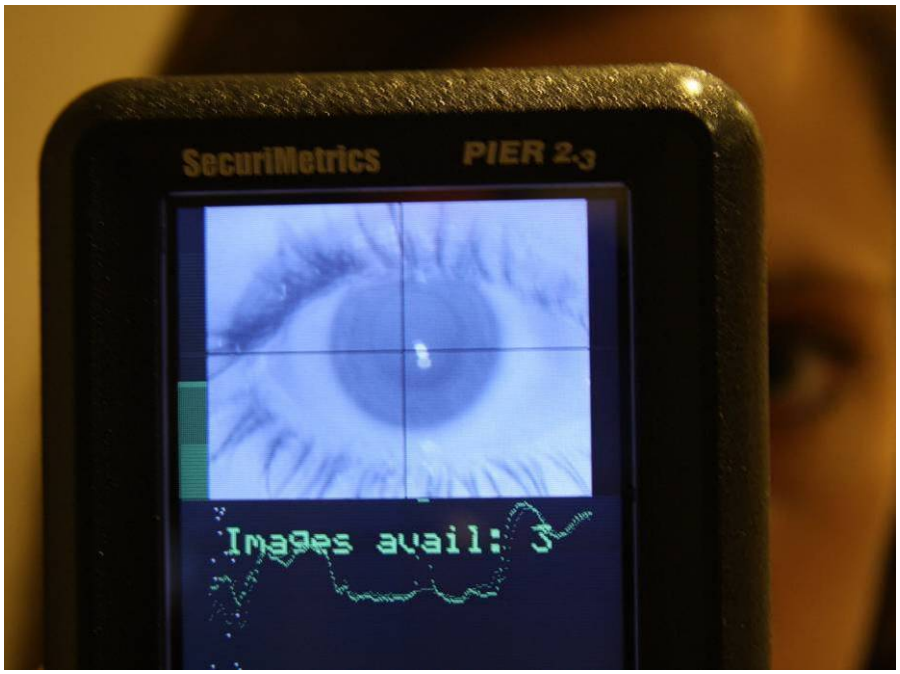


Figure 11. Above an iris is being scanned, note the green bar to the left of the image. The left bar indicated levels from 0 – 90% focus, with 90% being indicated by a green bar that extends the full length of the iris image. (image: Simon McLaren)

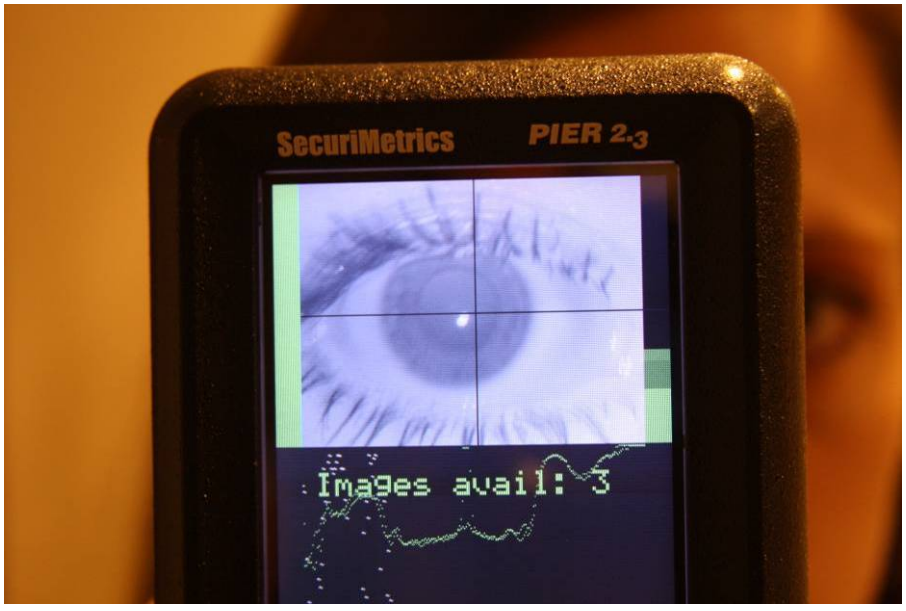


Figure 12. The image above shows an acceptable iris image as indicated by the full green bar to the left of the iris image and partial green bar to the right of the iris image. These green bars indicate the quality of the imaging being captured. It is desirable to collect images where at least a portion of the right green indicator is visible. (image: Simon McLaren)

b. False Rejection Rate

We experienced 6 false rejections out of 93 unique attempts, for a False Rejection Rate of 6.4%. Out of 25 subjects, 11 (or 44%) experienced at least 1 false rejection on a first attempt.

- Out of 100 attempts to recognize volunteers:
- 93 attempts were of registered volunteers
- 7 were of the spoiler

Two of the 25 subjects experienced only false rejections. Subjects 23 and 26 were never recognized by the PIER 2.3. Subject 23 only attempted to be scanned once during the experiment and the device failed to recognize the subject on either the first or second attempt. Subject 26 experienced a false rejection on the only attempt made to recognize him.

Overall recognition and rejection rates are a bit difficult to determine given the freedom subjects had to refuse a second or third attempt after a false rejection. No common protocol was administered with respect to a second attempt always following a false reject on a first attempt and a third attempt always following a false reject on a second attempt.

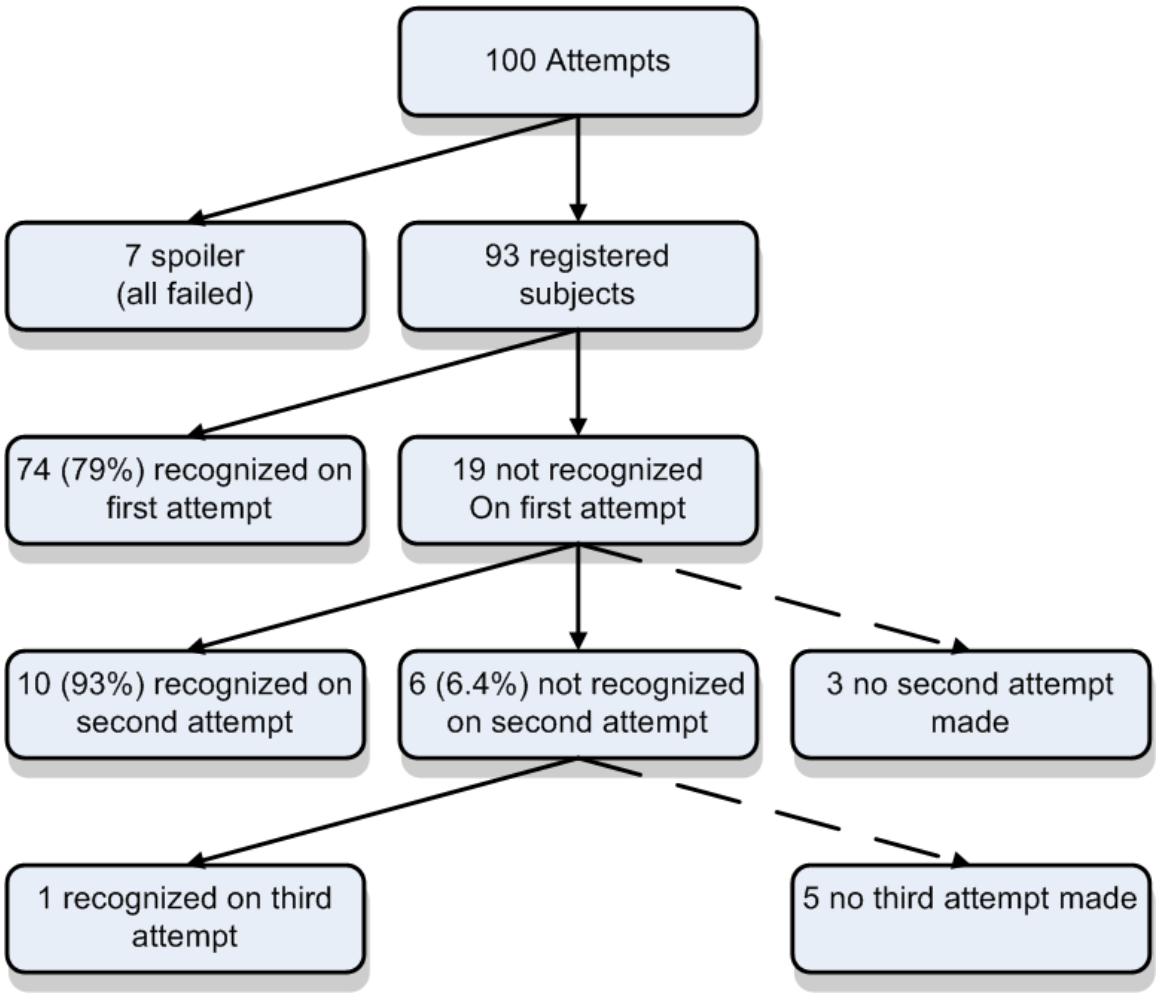


Table 37. Results of recognition attempts.

c. Attempts with Contact Lenses

Contacts lenses did not have a significant effect on the result of the experiment. First attempt successes were slightly higher for individuals who wore contacts during attempted scans.

Results of attempts on subjects who wore contacts during attempted recognitions:

- 11 attempts recorded
- 10 (91%) first attempt success
- 1 (9%) failed to recognize on either first or second attempt; did not receive a third attempt

Due to the low number of attempts made at recognition of individuals wearing contacts, the results were not statistically significant.

d. Attempts with Glasses

Wednesday thru Friday there were 6 attempts made to scan volunteer's irises while they wore their glasses. Of those 6 attempts 3 were successful. Of the three that failed with glasses on, 1 was successful when the glasses were removed, 1 was unsuccessful when the glasses were removed the last trial did not receive a second attempt.

e. False Acceptance

We did not experience a single false acceptance or misidentification during our experiment. All successful scans correctly identified the subject in question.

f. Overall Analysis

We believe that the FRR rate might be significantly improved through better training and monitoring of the operations. Many factors, including the angle of the device to the subject, have a critical effect on the performance.

While the operators were provided the recommended training, on average each guard only operated the device for a total of five hours during the experiment. It is likely that with continued use and a "refresher" training session to correct any incorrect operator tendencies, the observed error rates would decrease.

Given the relative position of the operator (standing) to the subject (sitting inside of vehicle) it should be anticipated that it will continue to be more difficult to position the device at a "correct " angle than if the operator and subject are positioned with eyes at the same elevation.

Our method did not remove trials from the results in cases where the operator may have incorrectly used the device (positioned the device at an angle too far off center or rotated too far from vertical) as this was a trial not only of the accuracy of

the device but an evaluation of how easy it was to learn to use the device. A longer trial period would be better suited to evaluate the reduced FRR expected with increased operator "familiarity" with the device.

The factor of the angle of the device relative to the subject is particularly relevant when scanning through eyeglasses, where management of that angle can reduce or eliminate the amount of glare or reflection cause by the eyeglasses reflecting both ambient light and the IR illumination of the device itself. While SecuriMetrics has designed the PIER 2.3 IR illuminators to shine toward the eyes at an angle that does not usually produce any reflection in the direction of the PIER lens, the addition of eyeglasses, which the subject may not always wear in a manner where the lenses is perpendicular to the surface of the eye, has the potential to inadvertently reflect the IR illumination into the device's camera lens.

2. Observed Time to Scan

Time-to-scan reported by the operators ranged from four to fifteen seconds, with a reported average of six seconds per scan. This was an average of the time required to scan the participants as reported by the scanner operators. An additional three to five seconds was then required for the scanner operator to visually verify the identity the scanner resolved to and the driver of the vehicle.

Drivers were required to come to a complete stop for the scanning to take place. This added an additional 10 to 20 seconds to the entry time at the gate. However, drivers are presently required to stop and undergo and ID check with the guard manning the gate. If the scanning had been conducted by this guard, rather than by an operator at a secondary location, there would have been no additional time added by the stop itself.

3. General Observations of Experiment Results

Overall, the experiment went well considering the number of adverse issues we experienced.

a. Specific Subjects Who Experienced Low Success Rates

Over half (13) of our subjects never experienced a false rejection during the field trial. Out of the 52 attempts at recognizing these 13 subjects, all 52 attempts succeeded on their first try. However, four of our subjects experienced false rejections requiring second attempts on 50% or more of their first attempts. While some of these failures might be explainable by the environment, at least one subject commented that she "seemed to always get rejected" by the device. This leads to some individuals, most likely based on physical attributes, experiencing false rejection more often than others. This is similar to the nondemocratic success of speech recognition systems that Doddington noted in 1998 [47].

b. Sunlight Backlighting the Subject

One of the volunteers experienced a false rejection on the first attempt when they walked up to the operator. The operator noted that the sun was directly behind the subject, which is a condition the manufacture trains the operator to ovoid. A bright light behind the subject creates an image that is back-lit and can significantly reduce the quality of the image captured by the iris scanner. The operator reported changing the relative position of the subject with respect to the sun and the second attempt result in a correct match.

c. Sunlight in the Face of the Subject

A second, unanticipated scenario occurred when the sun was low on the horizon and directly behind the operator. This placed a good deal of bright light directly into the face of the subject and resulted in at least 3 false rejections. The day 1 operator quickly adapted to this situation by placing his body between the sun and the subjects, thereby casting his shadow on the face of the subject on subsequent scans. The adaptation eliminated the bright light in the faces of the subjects, and improved the success rate of the scanner. The day 1 operator passed along his experience and solution to the rest of the operators, who then incorporated the solution when they operated the scanner.

There are three potential causes for bright light in the face of the subject causing increased false rejections.

- Too little iris visible: The bright light in the face of the subject might have caused the subject to squint. This would have resulted in a much greater portion of the iris being occluded, and there not being enough iris visible to the scanner to get a match.
- Too much iris visible: The bright light in the face of the subject would likely cause the pupil of the iris to contract. This would have resulted in more of the iris being exposed, and there not having been enough of the iris visible at the time of registration to produce a match.
- Glare: The bright light in the face of the subject might have produced a significant glare on the reflective surface of the iris. This would have resulted in an occlusion of a portion of the iris in the image that was captured by the scanner.

Regardless of the physical connection between the sunlight shining in the face of the subject, its affect on the pupil, eyelids, or surface reflection of the eye, and the impact on the image collected by the iris scanner; the solution was to block the source of light. In an office environment the light source can be repositioned so it no longer causes interference. This could be an issue in an outdoor mounted scenario where the iris scanner is collecting images of the iris at a distance.

If the TWIC program were to use iris scanning, the issue of sunlight might be a problem. The sun might be low on the horizon and shining directly into the faces of the drivers as they pass through the gate or are stopped to provide their job order to the port clerks. To compensate for this it might be necessary to build a sun shield behind the iris scanner to prevent the sun from directly shinning too brightly into the face of the driver whose iris would need to be scanned.

d. Relative Position of Operator and Subject

The correct relative position of the scanner in relation to the subject was difficult to maintain given the relative position of the operator (who was standing) to the subject (sitting inside of the vehicle). In these relative positions, which are natural given the guard and subject in vehicle scenario, the operator must lower the device well below their own eye level to align the device with the eye of the subject. This results in either

the device screen being more difficult to see for the operator as they must now view the screen at an angle above or alternatively to keep the screen at an optimal view angle, this forces the operator to place the device in a position where the camera lens in no longer vertical. Both of these scenarios become more pronounced as the relative eye elevation of the operator and subject become more uneven.

This can create a situation were the surfaces of the eye and iris camera lens are no longer parallel to one another, the position in which the scanner works best. This “incorrect” or suboptimal position is further complicated by a subject who is unable, or unwilling to position their head in such a manner to help make these two planes parallel. It may be physically difficult for a driver to both turn their head to the side while at the same time elevating their chin high enough to position their eye such that the surface is now parallel with the front surface of the scanner device.

One method to overcome this would be for the operator to kneel or bend down to position themselves with their eye level more closely matching the eye level of the subject being scanned. However, even if this were to reduce the error introduce by a mis-positioned scanner, it is hardly a comfortable solution for an operator.

However, this is simply an observation from the overall results of the experiment, and no analysis has been done to determine the amount of error this less than optimum relative position of the operator and subject may introduce to the process.

Another potential solution to this dilemma may already exist, the 2007 Daugman algorithm discussed in chapter two. This newer algorithm is supposed to handle this less than optimal position of the eye to the scanner, commonly referred to as an off-axis scan., although the term “off nadir” may be more appropriate.

Our method did not remove trials from the results in cases where the operator may have incorrectly used the device (positioned the device at an angle to far off center or rotated too far from vertical) as this was a trial not only of the accuracy of the device but an evaluation of how easy it was to learn to use the device. A longer trial period would be better suited to evaluate the reduced FRR expected with increased operator "familiarity" with the device.

The factor of the angle of the device relative to the subject is particularly relevant when scanning through eyeglasses, where management of that angle can reduce or eliminate the amount of glare or reflection cause by the eyeglasses reflecting both ambient light and the IR illumination of the device itself.

e. Concerns About the Potential Physical Injury Iris Scanner May Cause

During the recruiting phase for this experiment, I spoke with many potential volunteers and FNMOC as I toured the facility and spoke with friends and previous co-workers about possibly volunteering. More than a few of those who volunteered were initially hesitant to participate stating they were concerned about potential physical injury the iris scanner might cause. This fear was both about the potential for injury over even a short term exposure to iris scanning as well as the potential cumulative effects it might have. This experience is not unique to our pilot study as usability study of biometrics with ATMs also encountered this concern [54].

Some people remained concerned even after they were told that an iris scanner is really nothing more than a camera, and if they have ever played with a home video camera that has a night vision feature, they had been exposed to infra-red light similar to what the PIER 2.3 uses. This concern highlighted the general unfamiliarity the public has with iris recognition and the potential to confuse it with retina scanning. While it is possible that some of these acquaintances were simply looking for a convenient excuse to not participate, it suggests that potential pools of subjects would need to be educated to overcome the possible misconceptions with regard to the minimal health risk iris recognition systems present.

It also suggests that when introducing iris recognition to new groups of users who are previously unfamiliar with the technology, it could be prudent to avoid describing the process as “scanning.” Scanning seems to intuitively imply that the body is being bombarded with some form of electromagnetic wave that “certainly” must pose some health risk – no matter what someone else tells you.

f. Concerns About Providing a Biometric to a Government Official

Other non-participants interviewed expressed their concern of providing their iris template to a government official; even if it was just for a thesis experiment. In spite of assurances that the iris template collected for the experiment would be destroyed at the end of the experiment, some individuals were still so cautious about giving up their "image" that it prevented them from participating.

This highlights the mistrust some Americans have of their government. It was somewhat surprising to see this mistrust from individuals who worked for and received their livelihood from the DoD. This highlights the need to provide individuals who may be forced to utilize such devices with assurances of how their biometrics will be used. Maybe more importantly, is the need to educate them on the consequences the government would face if their biometric data is used for a purpose other than which it was originally intended.

The government can promise it will not misuse information collected about its citizens, but without educating those citizens on what safeguards are in place to prevent its misuse or loss, and what consequences await a government official who would knowingly use that information for another purpose, the government has little hope of calming those fears.

g. Observations of the Training Methodology

Following the experiment we were able to debrief the scanner operators. All noted that the training they had received was adequate and that the device was intuitive to use when being run in recognition mode. The three operators who viewed the manufacture provided training DVD stated that the DVD based training provided ample visual demonstration, if not somewhat repetitive.

All four operators felt that while the DVD training was nice, the hands-on training period was more useful as it allowed them to put what they had observed on the DVD to practice, and that by doing so made it much easier to remember than simply

watching a video. They all felt that the hands-on training by itself was sufficient to learn how to use the device. One operator did comment that the repetition in the training video was useful.

h. Scanning Through Corrective Lenses

Unfortunately, the experiment only resulted in six attempts to scan through corrective lenses (eye glasses). Of the six glasses on attempts at recognition made, two attempts resulted in successful recognitions.

Of the four attempts that failed through the glasses, two were successfully recognized when a second attempt to scan their eye was made immediately without the glasses. One glass-on failure did not receive a second attempt without glasses. This was one of the challenges that were observed with this field experiment, subjects were free to refuse recognition attempts at any time and for whatever reason.

The last individual who experienced a failure with glasses on also failed to be recognized when a second attempt at recognition immediately followed without glasses. This individual had been recognized before both with glasses on and without glasses.

One of the operators did note that provided you did not have a glare on the surface of the glasses the device seemed to work well. The author noted in pre-experiment familiarization and during the registration process that the infra-red illuminators of the device itself could cause a glare on eye glasses. This was usually overcome with relative ease by simply taking the iris scan at a slight left or right angle to the perpendicular of the glasses themselves.

i. Usability of the PIER 2.3

The operators of the PIER device provided very positive feedback concerning the ease of use and relatively intuitive interface of the PIER 2.3. Three of the

operators commented on the touch screen interface and that they found it very "nice" to use. However, all four operators, when specifically asked, provided recommendations to improve the user interface.

4. Suggestions for Improvement of the PIER 2.3 from Operators

The scanner operators were debriefed at the end of the experiment to gather feedback about their experience with the PIER 2.3 and possible areas of improvements to the device. As with almost all users of "high tech" toys, when asked, have a lot of suggestions for improvement; and the operators for this experiment were no different. Here are the suggestions the operators provided:

a. Single Button to Recognition Mode

Since the device is used more often in recognition mode, (according to our operators) it would be useful to have a single button on the device that set the device in recognition mode directly and that did not require navigation of multiple menu options. The PIER 2.3 currently requires the operator to navigate to the recognition mode. While this navigation only requires the operator to press two buttons or two equivalent touches of the touch screen, that requirement was found to be inconvenient particularly in combination with the next area of potential improvement.

b. Longer Wait Prior to Auto Power Down

The operators also noted that the timer on the device to power down automatically was set somewhat short. The operators noted that during time of low gate-crossing volume, the device would almost always power down between recognition attempts. While the PIER 2.3 powers up in approximately 15 seconds, this additional 15 to 20 seconds wait spent powering up and navigating to the recognition mode would nearly double the total time required to process a subject. While the operators understood that the auto power-down feature was intended to extend battery life, they still found it to be inconvenient.

c. Screen Brightness and Reflectivity

The operators also noted that at times the screen of the PIER 2.3 was difficult to see in bright sunlight and that this could be improved on to make the device more "friendly" in outdoor applications. This suggestion of course also finds itself in opposition to extending the battery life of the device. In bright sunlight this situation is further exaggerated by the reflectivity of the screen itself. The operators also thought a low gloss screen would improve the ease of use in outdoor applications. This combination became a considerable issue when the sun was directly behind the operator, with one operator stating that at times this prevented him from being able to see the screen well enough to "put the x on the eye" of the subject. This may have contributed to the 26% first scan false rejection rate experienced.

d. Reduce Required Proximity to Face

The operators also mentioned that at times they observed subjects acting uncomfortable when the device was moved closer to their face in order to capture an iris scan. The distance of 4"- 8" was often felt to invade the personal space of the subject being scanned. This might be a cultural concern as Americans tend to expect a large area of "personal space" around their person than other cultures do. One of the operators also commented "since when is security supposed to be comfortable. Maybe in this situation a little invasion of ones personal space is ok."

SecuriMetrics' newer HIIDE Series 4 device has a focal length of 8 – 10 inches, which reduces the intrusion into personal space the operator must make to obtain an iris image from the subject.

e. Make it More Ruggedized

One more possible improvement the operators provided would be to add "rubberized sides" to improve the grip of the device. Along with the rubberized sides the operators also thought rubber stoppers on the backside of the device would also help to protect the PIER if it were laid down, particularly on a slick and slightly slanted surface.

5. Suggestions for Improvement of the PIER 2.3 From Author

A few more possible suggestions for improvement of the PIER 2.3:

a. Onboard Template Fusion

One of the shortcomings of the device was evident only during the registration process. Biometric Fusion, or being able to tie multiple biometric templates to a single record or body, was missing in the PIER 2.3. With the PIER 2.3, each eye was registered and created a unique entry in the onboard database in the PIER 2.3. If care was not taken during enrollment, it was possible to give the same body two names in the database, one for each iris. SecuriMetrics does produces software for more robust template databases to be used in conjunction with the PIER 2.3 and other SecuriMetrics devices and this addresses the problem when the software is available on a desktop or laptop during registration. SecuriMetrics has also addressed this issue in more recent handheld iris devices, but if a software upgrade were provided for the PIER 2.3, this would be an area for improvement.

b. Faster Frame Capture Rates

One possible cause for the high first attempt false rejection rate experienced in this experiment (26%) could be the frame rate of the device. The current frame rate of 15 frames per second may introduce less reliability in capturing images that are in focus simply due to hand shake of the operator. This potential effect would be greatly diminished for any stationary application of an iris scanner, but for handheld devices a faster shutter speed might help to improve first attempt successes. This would not only offset hand motion, but could also offset motion of the subject being scanned.

c. Image Stabilization of Camera

A second option might be to add image stabilization similar to the type that has recently become available on even relatively inexpensive video and digital cameras. Taken in conjunction with faster frame rates mentioned above, this could have a considerable improvement in image focus during capture.

d. Adjustable Angle View Screen

In our application, the relative position of the operator (standing) to the subject (sitting inside of vehicle) caused some difficulty in correct positioning of the device relative to the subject. This situation might be addressed by adding a view screen where its angle can be adjusted to allow a better view for the operator (similar to most video cameras), when the device is not used at the eye level of the operator. In our scenario with the operator (standing) to the subject (sitting inside of vehicle) the operators often had to use the device in a position well below their own eye level. This situation introduced some additional difficulty in proper alignment of the device relative to the subject's eye that is not experienced when both subjects' eyes are much closer to the same elevation.

E. RELEVANCE TO THE TWIC USAGE SCENARIO

1. Sunlight is a Factor

One of the unanticipated discoveries of the experiment was the role sunlight played on the success of the recognition attempts when the sun was directly behind the scanner or individuals operating the scanner. This situation put the sunlight shining directly into the face of the subject. During this field trial we experienced considerable difficulty in this scenario. The operators' corrective action was to place their body between the sun and the subject, thereby casting a shadow over the face of the subject. This simple action resulted in at least three documented successful second attempts during the field experiment. It is also likely this action contributed to many successful first attempt successes.

When iris scanners are deployed to outdoor applications similar to the scenario of this field experiment, it will often be the case that it is cost prohibitive to undertake construction to redirect the direction of traffic to prevent the sun ever shining directly into the face of the subject being scanned. In these instances, consideration should be given

to either place the iris scanner in a deferent location, if possible, or to provide a shade of some sort to block the sun from shining directly into the face of the subject being scanned.

Possible solutions here would be to build walls between lanes of traffic to provide that shade, or to simply place a large sun-block behind the iris scanner in the form of a metal plate or other reasonable rugged sheet.

2. Eyeglasses are a Factor

This field experiment recorded some successes of iris recognition even when the subject did not remove their eyeglasses; however, this was more of an exception than the rule. Even though the experiment did not provide enough scans in this scenario to be able to make statements of statistical significance about eyeglasses, it is likely that the effect of glasses will be a factor in the deployment of iris scanner in any scenario where scans are conducted on subjects while they are in their vehicles. Some drivers are unable to drive legally without wearing their eyeglasses and as such it should be expected that these drivers will be a part of the population to seek entry at any facility where iris scanning at the "gate" is implemented.

This can be addressed easily enough through education and in the case of Ports, by reminders made by the gate guard or the clerk who processes the business transaction of the drivers, depending on where the iris scanner might be installed.

F. SHORTCOMINGS OF THE EXPERIMENT CHECK

During the course of the experiment we were unable to test under a number of conditions that are likely to be experienced in any real-world manned or unmanned gated facility scenario. While the PIER 2.3 would not lend itself to an unmanned application, it did provide some insight to the over-all gated facility application. Eventually we would envision gated facilities utilizing an automated iris scanner that is designed to handle traffic much like the latest device which was introduced to the world by Sarnoff Corporation [25].

It would have been more realistic to have attempted a field test of the Sarnoff solution [25], however as this device was only released in November of 2007 this was not possible as this field experiment was being arranged well before that time.

We did not operate this experiment during times of low light conditions similar to those experienced during late evening or night time. Many U.S. shipping port operate around the clock and any application of iris scanners at the gates of these facilities would need to operate under these conditions.

Throughout the duration of this experiment we did not encounter periods of high humidity or dense fog or any other extreme weather condition. For an iris scanner to be practical for deployment in the unmanned scenario to screen drivers at a gated port facility, it will need to operate 24 hours a day 365 day a year. This will include extreme weather conditions including rain (light to heavy), fog (light to dense), snow, extreme winds, high dust levels and combinations of these. These weather conditions are likely to present an issue for any iris scanning device, but particularly a mounted and unmanned device that cannot be "brought in from the rain", so to speak, when the weather conditions are less than favorable.

During the experiment, we operated the PIER 2.3 in a one-to-many identity establishment mode. The TWIC program is intended to utilize the TWIC card to provide a claimed identity and use the biometric device to verify that identity with respect to the individual who presented the TWIC card. We did not test in this configuration, but it would seem to be less demanding than the one-to-many scenario.

This pilot experiment was conducted with a very limited pool of 25 individuals with two iris templates for each (except the spoiler). Any real-world application will need to handle hundreds or thousands of templates. We did not simulate this level of templates as potential mismatches. While research indicates that these vastly larger numbers do not significantly increase the likelihood of false accepts [41], it would still be prudent to test this in field conditions.

This experiment took place over a short time period of two weeks. It would be prudent to conduct an experiment that covered a much more significant period of time.

False rejections did not all receive the same level of follow-up attempts. This was often due to the flow of traffic or the impatience of the test subject. A more uniform handling of false rejects might have provided a better understanding of multiple attempts.

During this experiment one individual served as both the operator and recorder. This occasionally placed the individual in a position to have to choose between providing detailed notes and scanning the next subject in the queue.

G. FUTURE WORK

1. Experiment Improvements

A follow-up experiment could be improved in the following ways:

- Improved application of a standard protocol when it came to handling first and second attempt failures. It would be beneficial to ensure as much as possible to ensure all recognition attempts received an equal number of attempts at recognition before being called a false reject.
- Test the device in low-light conditions such as those found during dusk to nightfall and during the night time. This would provide an understanding of how dilated pupils might affect the efficiency of the device. Again, registration should be done in atypical office-like conditions and the full range of outdoor lighting conditions should be tested.
- A repetition of this experiment would be better suited toward using the new Sarnoff "Drive-Through" system [25] or a similar device. This will provide an evaluation of an unmanned solution as this would most like be the type of device desired at a gated facility.
- Testing of the device in extreme weather conditions to include rain, snow, fog, dust, high winds and combinations of these. Unmanned, mounted devices should be tested by allowing them to remain exposed to these conditions for prolonged periods to mimic the 24/7, 365 days a year operations of many U.S. shipping ports to ensure the devices are both

durable and can indeed operate in such weather conditions. During any prolonged exposure to the elements, any mounted device is likely to experience film build up of dirt and grime from oil sourced in the facility, as well as snow and ice build up during winter conditions. These scenarios must be fully tested with favorable results (or at least more favorable than alternative biometric options) before iris scanners could be the solution of choice for this scenario.

- The device should be tested in an identity establishment mode as well as an identity verification mode.
- There is opportunity to design a proto-type for interfacing the TWIC card to provide a claimed identity and the device to verify that claimed identity.
- This experiment should be repeated with hundreds of thousands of iris templates loaded into the database to simulate the large number of templates likely in a real-world deployment of iris scanners. This could be accomplished by preloading the template database with other "real" templates. These are available.
- This sort of field experiment should test the stability of the irises test population over a longer period of time. A time frame of three years would be sufficient to show that the iris is stable under fielded conditions. Beyond this time frame would not be necessary, as the TWIC card itself must be renewed on a regular time frame (five years) and the digital ID's on the card must currently be renewed every three years. These events both present opportunities to collect a new biometric template at regular intervals, even if some individual have less stable iris patterns. Although this is not expected to be an issue, as the iris tends to achieve stability very early in the development of the human body [48].
- In a repeated experiment, it would also be wise to monitor the operators to look for operator actions that introduce error and reduce the accuracy of the device during capture of the iris image.

- It would also be prudent to conduct the experiment with an additional "record keeper" who would record event and notes on conditions that might contribute to false rejections. This would most likely result in more detailed notes about false rejections. During this experiment, one individual served as both the operator and recorder. This occasionally placed the individual in a position to have to choose between providing detailed notes and scanning the next subject in the queue.
- Replacing the PIER 2.3 with the SecuriMetrics HIIDE device to test the affects of the newer Daugman 2007 iris recognition algorithm on the off nadir alignment that seemed common when the relative eye levels of the operator and subject were different.

Many of these recommendations could be easily fingerprint scanning. In the future, DHS or some other organization might try to directly compare different biometric technologies before issuing recommendations mandating a specific technology.

V. SUMMARY AND CONCLUSIONS

A. SUMMARY OF OBSERVED RELIABILITY OF PIER 2.3

Overall we were very pleased with the PIER 2.3 device and felt it performed very well in our pilot field study. While we experienced a higher False Rejection Rate than is common for iris recognition devices; this was most likely due to operator actions. We did come across two conditions that seemed to increase the overall False Rejection Rate experienced during the field experiment.

We experienced conditions where the sun was low on the horizon and positioned behind the back of the PIER operator. This allowed the sun to shine brightly and directly into the faces of the subjects being scanned during the morning hours of the experiment. The result was an increased occurrence of false rejections. This could be due to direct effects of sunlight, i.e. reflecting of the surface of the eye or constricting of the pupil resulting in exposure of more iris surface to the camera. It could also have been a been due to less direct effects of the direct sunlight, squinting by the subject in reaction to the direct sunlight, reflection of the screen of the PIER 2.3 view screen making it more difficult to properly align the device to capture an iris image, or any combination of these direct and indirect effects.

Regardless of the link between the direct sunlight into the face of the subject being scanned, the solution was to block the direct sunlight by casting a shadow over the subject's face and the view screen of the PIER 2.3 device. In this experiment this was accomplished by the PIER 2.3 operator repositioning their body to cast that shadow.

A second potential cause of the increased False Rejection Rate may have been ergonomics and relative position of the operator with respect to the subject. When the PIER 2.3 was used to obtain an iris image of a subject that was sitting in a low vehicle, this placed the operator and the subject's shoulders at different elevations. This in turn meant that as the operator lowered the PIER 2.3 in their hand to the level of the subject's eye, the hand followed an arcing motion which caused the PIER to no longer be in a

vertical position. In some cases, the subject inside the vehicle was able to tilt their own head in such a way as to maintain proper alignment between the PIER 2.3 and their eye. In other cases the subjects were either unaware of the need or physically unable to achieve the required relative alignment. The newer Daugman 2007 iris recognition algorithm may be able to compensate for this misalignment, as it's specifically intended to "correct" for off nadir scans of the iris.

Both of these issues could have an impact on future deployments of iris scanners to screen drivers of vehicles while they are still inside of their vehicle. While an unmanned application of an iris scanner may address the sunlight reflection of the view screen issue, it would still be vulnerable to the effects of the direct sunlight on the subject's iris itself and increased squinting. In addition a fixed mount iris scanner is likely to further complicate the relative positioning and alignment of the scanner and the iris in scenarios where vehicle height is variable as might be expected at a port facility where both passenger vehicles and tractor-trailers must be screened at the same gate.

B. SUMMARY OF BIOMETRIC ATTITUDES SURVEY

The Biometric Attitudes Survey indicated three important issues for consideration by policy makers:

1. No Biometrics Where Identification is Not Currently Required

The survey showed a rather high degree of support of the use of biometrics in scenarios where positive identification is required today, such as gun sales and traffic stops. The introduction of biometrics into these scenarios only changes the method by which that identification is presented. None of these scenarios introduced a new requirement for positive identification.

Facial recognition received lower levels of support in general than fingerprint identification. This may very well be due to the perceived clandestine nature by which facial recognition works. From both the qualitative survey results and the opened comments, individuals seem opposed to not being able to control the presentation of their identities. The 2001 survey conducted by Opinions Research Corporation [15] strongly

suggested this, with 95% of their respondents finding it important that "an individual should be told whenever his biometric identifier is being collected – it could not be collected secretly" except in national security situations. Individuals also seem to desire the ability to maintain some level of anonymity in scenarios where their identification is not required by today's laws.

Survey respondents found the scenarios that suggested the use of biometrics to establish identity where it is not already required today, to be significantly less acceptable. This would seem to strongly indicate that the perceived invasion of privacy takes place mainly when there are attempts made to identify individuals in scenarios where they are able to be anonymous under current requirements.

2. Individuals Do Not Trust the Government

Only 22% of individuals who responded stated they trusted the U.S. Government to not misuse biometric data it collects. This seems fitting with the tradition of Americans throughout our history. Our founding fathers sought to limit the power of government and in particular our federal government. It could be that this tradition still holds strong today and that most Americans do not trust the government to stay with in its bounds.

Opinions Research Corporation found that 97% of it respondents thought it was important that "An organization collecting biometric IDs should not use them for any other purpose other than those originally described to the individual, unless required to do so by law or each person in the system has been informed and given their consent." [15]

One way to address this is for the government to educate the public on the penalties a government official will face if these collected biometrics are misused. The public is not likely to trust the government unless they understand the incentive government officials have to live within the law.

3. Do Not Tread on Spiritual Beliefs

Many survey respondents indicated they held strong religious beliefs that the Biblical "Mark of the Beast" is real, and will come to fruition at some point in the future. Many have a strong fear of biometrics fulfilling that prophecy. Regardless if these people are right or wrong, consideration must be given to those individuals who have those beliefs. With specific regard to the "Mark of the Beast", care must be taken to understand what these individuals are likely to interpret as fulfillment of prophecy, and policies that would "fit" should be avoided.

In the Bible, the Mark of the Beast is described as the addition of some form of identifying mark to the individual. In contrast, biometrics are the measure of what an individual is already, i.e. individuals already posses their biometric at birth.

C. POLICY IMPLICATIONS

1. Avoiding the Mark of the Beast

"I think of it as fulfilling prophecy from the book of Revelations in the Bible." This was one response from the survey respondent when asked if they had any moral or religious concerns about the use of biometrics. Another respondent replied, "I tend to view it as inevitable. Human nature being what it is/prophecies having been made 1000's of years ago, I know they will eventually be greatly misused." A third responded, "Only if a device is imbedded into the forehead or wrist for identification."

All of these responses are clear references to the Revelations 13:16-18, which indicates that all people on the earth will be required to take the "Mark of the Beast" to be able to function in society during the period referred to as the "Great Tribulation" that is prophesied to take place during the last seven years of life as we know it on earth.

> Revelations 13: (v16) And he causeth all, both small and great, rich and poor, free and bond, to receive a mark in their right hand, or in their foreheads: (v17) And that no man might buy or sell, save he that had the mark, or the name of the beast, or the number of his name. (v18) Here is

> wisdom. Let him that hath understanding count the number of the beast: for it is the number of a man; and his number is Six hundred threescore and six. (King James Version)

One clear implication here for future governmental policy surrounding the use of biometric and other identification programs is the need to take proactive action to avoid the program being viewed in the context of the "Mark of the Beast." The description of the mark in the Bible indicates that it will be "in their right hand, or in their foreheads." Given that a recent Time/CCN poll "found that 59% of Americas believe the events in Revelations are going to come true", [60] creating government policy today to prevent the use of these two areas of the human body from being used for identification purposes, might go a long way to minimize the concerns of those individuals who believe strongly in a literal interpretation of this portion of the Bible. This might have a larger implication with RFID implanted chips than biometrics, or implanted RFID chips used in combination with biometrics, but even so great consideration must be given to those who believe.

2. Limit New Identification Requirements

The Biometrics Attitudes survey showed that respondents tended to find the use of biometrics to confirm or establish a person's identity to be acceptable when it was used in a scenario that requires positive identification today. Examples include interactions with law enforcement, firearm sales and access to classified information. When the scenarios described included the use of biometrics to establish an individual's identity in scenarios that are not required today, there was much greater level of resistance to such applications.

This suggests that policy makers should look to use biometrics to help enforce current legal requirements before looking for "new" applications of strong identification in society.

3. Clearly State Biometric Data Protection Policy and Penalties

The concerns voiced by the ILWU representative about possible use of biometric data in ways not originally intended are hardly unique. The ORC survey demonstrated a clear public sentiment that government is likely to expand the use of any data it collects beyond its original intended purpose. One thing the survey of attitudes and comments from respondents made clear it that individuals are less concerned with the technology of biometrics than they are with it potential uses. The majority of the survey respondents to not trust that government will not "misuse" this information. However, there is no definition of what is "misuse." Some suggest that any use beyond the stated specific purpose would be misuse; others would be more open and allow for some degree of expanded use. Almost all agree that at some point the information could be used in an unacceptable manner.

To avoid public outcry and objections to the actions of government, our elected officials may need to take action to define what acceptable uses of biometrics are by enacting laws that prevent "mission creep" of biometrics, and limiting the uses to only those uses that subjects were informed of and agreed to at the time of collection. This seems to be even more important as a limitation of government programs and their use of biometrics than it might be in the private sector.

LIST OF REFERENCES

[1] US. Department of Homeland Security. “DHS Must Address Significant Security Vulnerabilities Prior to TWIC Implementation.” [Washington D.C.]: The Department, 7 Jul 2006.

[2] “Transportation Worker ID Card Riddled with Privacy and Security Holes” *Spotlight on Surveillance* Jul 2006 Electronic Privacy Information Center. Jul 2006, [cited 28 Aug 2007], Available: http://www.epic.org/privacy/surveillance/spotlight/0706/.

[3] US. Government Accounting Office. “GAO-07-681T. Hearing on “Transportation Security: TSA Has Made Progress in Implementing the Transportation Workers Identification Credential Program, but Challenges Remain,” 12 Apr 2007, Available: http://www.gao.gov/new.items/d07681t.pdf.

[4] American Association of Port Authorities. “Comments on Transportation Worker Identification Credential Implementation in the Maritime Sector.” Alexandria, VA, 30 Jun 2006.

[5] George P. Cummings, Director of Homeland Security for the Port of Los Angeles, “Testimony before the U.S. Senate Committee on Commerce, Science and Transportation” 16 May 2006. [cited 18 Nov 2007], Available: http://commerce.senate.gov/public/_files/cummings0516060.pdf.

[6] George P. Cummings, Director of Homeland Security for the Port of Los Angeles. Telephone interview. 11 Sep 2007.

[7] L-1 Identity Solutions, “L-1 Identity Solutions Releases Latest Daugman 2007 Algorithm for Highly Accurate Iris Recognition in Challenging Environments” 01 Aug 2007. Press release.

[8] Daugman, John G. "High Confidence Visual Recognition of Persons by a Test of Statistical Independence." IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 15, pp. 1148-1161, 11 Nov 1993.

[9] John G. Daugman, “How Iris Recognition Works.” IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, pp. 21-30, 11 Jan 2004.

[10] U.S. Census Bureau, Estimated Population Clock, [cited 19:05 GMT 13 Jan 2008], Available: http://www.census.gov/main/www/popclock.html.

[11] U.S.. White House. “Homeland Security Presidential Directive/HSPD-12,” George Bush. 27 Aug 2004. [cited 15 Sep 2007], Available: http://www.whitehouse.gov/news/releases/2004/08/20040827-8.html.

[12] Paul. A. Karger, "Privacy and Security Threat Analysis of the Federal Employee Personal Identity Verification (PIV) Program" *Symposium On Useable Privacy and Security (SOUPS) 2006*, (Pittsburg, PA, USA 12-14 Jul 2006).

[13] U.S. Department of Commerce. National Institute of Standards and Technology. "Federal Information Processing Standards Publication 201 Change Notice 1," Mar 2006.

[14] Kevin Krick, Assistant Director, Security & Accident Prevention Pacific Maritime Association and Ed Hughlett, Manger Northern California Safety and Health Marine Terminal Corporation. Interview 19 Dec 2007 San Francisco, CA.

[15] Opinion Research Corporation International, "Public Attitudes Toward the Uses of Biometric Technologies." SEARCH.ORG, Aug 2002.

[16] Simson Garfinkel, and Beth Rosenberg, eds. *RFID Applications, Security and Privacy*. Upper Saddle River: Addison-Wesley, 2005.

[17] "Maritime Transportation Security Act of 2002" (PL 107-295) 25 Nov 2002.

[18] Colin Soutar, "Implementation of Biometric Systems – Security and Privacy Considerations." *Information Security Technical Report*, vol. 7. 4 Dec 2008, pp 49-55.

[19] "Recognition verses identity – the role of biometrics" *Biometric Technology Today*, vol. 11. 6 Jun 2003, pp. 7-8.

[20] TRUSTe "More than Tow-Thirds of American Support Adding Biometrics to Government Issued Identification," 9 Jan 2007, Press Release.

[21] G. Guo, M. Jones, and P. Beardsley, "*A System for Automatic Iris Capturing.*" Mitsubishi Electric Research Laboratories, Tech Rep. TR2005-044, 2005.

[22] Ulf M. Cahn von Seelen, Ted Camus, Peter L. Venetianer, Guanghua G. Zhang, Marcos Salganicoff, and Michael Negin: "Active Vision as an Enabling Technology for User-Friendly Iris Identification." *2nd IEEE Workshop on Automatic Identification Advanced Technologies*, (Summit, NJ, 28-29 Oct 1999, pp. 169-172).

[23] Ulf M. Cahn von Seelen: 'Countermeasures Against Iris Spoofing With Contact Lenses.' *Biometric Consortium Conference BC2005*, (Arlington, VA, 19-21 Sep 2005).

[24] Sarnoff Corporation. Advertisement. 2006, [cited 14 Jan 2007], Available: http://www.sarnoff.com/downloads/products/iris-on-the-move/portal_system_specs.pdf.

[25] Sarnoff Corporation "Sarnoff Corporation Unveils Latest Technology for Access Control" 11 Jan 2004. Press Release.

[26] Barry Fox, "Invention: Covert Iris scanner" *New Scientist Tech.* 05 Feb 2007, [cited 15 Jan 2008].

[27] John Daugman, "Biometric personal identification system based on iris analysis." U.S. Patent 5,291,560. 1 Mar 1994.

[28] "Privium – A select way to travel." Amsterdam Airport Schiphol 2008, 21 Jan 2008 [cited 21 Jan 2008], Available: http://www.schiphol.nl/privium/privium.jsp.

[29] John Daugman, "John Daugman's webpage" University of Cambridge [cited 21 Jan 2008], Available: http://www.cl.cam.ac.uk/~jgd1000/.

[30] UK. Immigration Service. Home Office. "Project Iris – Pilot Review Report V 3.0" 30 Nov 2006.

[31] UK. Home Office. Border and Immigration Agency "IRIS – Iris Recognition Immigration System," [cited 21 Jan 2008].

[32] "Jakarta airport debuts iris scanner to speed travelers" *Reuters*, 21 Dec 2006, [cited 22 Jan 2008] Available: http://www.reuters.com/article/worldNews/idUSJAK13330820061221.

[33] "Selected Case Studies" Iridian Technologies. Website [cited 22 Jan 2008]. Available: http://www.iridiantech.com/solutions.php.

[34] "Frankfurt Airport's BioP II trial unveils unexpected results" *Biometric Technology Today*, vol. 13, pp. 1, 9 Oct 2005

[35] "Iris recognition excels in refugee scheme" *Biometrics Technology Today*, vol. 13, p. 5, 5 May 2005.

[36] C. Carey, "Iris scan gives positive IDs of prison inmates." *Access Control and Security Systems Integration*, 42(1):18. 1999.

[37] "New Partnership Will Create National Database to Identify Missing Children" The CHILD Project 9 Feb 2004, [cited 22 Jan 2008], Available: http://www.thechildproject.org/press/pr_2004-02-09.html.

[38] P. J. Phillips, W. T. Scruggs, A. J. O'Toole, P. J. Flynn, K. W. Bowyer, C. L. Schott, and M. Sharpe, "FRVT 2006 and ICE 2006 Large-Scale Results" National Institute of Standards and Technology. 29 Mar 2006.

[39] Daugman, John "Probing the Uniqueness and Randomness or IrisCodes: Result from 200 Billion Iris Pair Comparisons" *Proceedings of the IEEE*, Vol 94, 11 Nov 2006.

[40] Cathy Newman, "A Life Revealed" *National Geographic Magazine,* Apr 2002. [cited 23 Jan 2008], Available: http://ngm.nationalgeographic.com/ngm/afghangirl/index.html.

[41] John Daugman, "The importance of being random: statistical principles of iris recognition." *Patter Recognition*, vol. 36, pp. 279-291, 2 Feb 2003.

[42] John Daugman, and Cathryn Downing, "Epigenetic Randomness, Complexity and Singularity of Human Iris Patterns" *Proceedings: Biological Sciences*, Vol. 268. No. 1477, pp. 1737-1740, 22 Aug 2001.

[43] U.S. Department of Commerce. Census Bureau "Earnings Gap Highlighted by Census Bureau Data on Educational Attainment" 15 Mar 2007. Press Release.

[44] Valorie S. Valencia, "Current State of Iris Recognition Performance: Image Quality and Interoperability." *Biometric Consortium Conference, Panel of Advanced Technologies for Iris Recognition*. Presentation. 12 Sep 2007.

[45] Simson Garfinkel, *Database Nation.* Sebastopol: O'Reilly & Associates, Inc., 2000.

[46] U.S.. Dept of the Treasury. Bureau of Alcohol, Tobacco and Firearms. ATF F 4473. [cited 1 Feb 2007] Available: http://www.atf.gov/forms/4473/.

[47] Doddington, Ligget, Martin, Pryzbocki and Reynolds "Sheep, Goats, Lambs and Wolves, A Statistical Analysis of speaker Performance in the NIST 1998 Speaker Recognition Evaluation" *Proceedings of the ICSLP*, v 13. pp. 1-5, 1998.

[48] P. Kronfeld, "Gross anatomy and embryology of the eye," in *The Eye, H. Davidson*, Ed. London, U.K.: Academic, 1962.

[49] SecuriMetrics "SecuriMetrics Hardware Products." Website [cited 04 Mar 2008], Available: www.securimetrics.com/solutions.

[50] U.S. Department of Defense. DefenceLINK News Photos Mar 2008 http://www.defenselink.mil/photos/NewsPhoto.aspx?NewsPhotoID=8775.

[51] Joel Abshier, “High-tech ID system sniffs out hidden threats.” *Marine Corp News.* Story ID#: 2007728516613 28 Jul 2007. Available: http://www.usmc.mil/marinelink/mcn2000.nsf/news.

[52] CLEAR web site. [cited Mar 2008]. Available: http://flyclear.com/index.html.

[53] John Daugman, “Iris recognition boarder-crossing system in the UAE.” *International Airport Review,* Issue 2. 2004.

[54] Coventry, Lynne, De Angeli, Antonella, Johnson, Graham. “Usability and biometrics at the ATM interface.” *Proceedings of the SIGCHI conference on Human Factor in computing systems.* ACM. Apr 2003.

[55] OKI “OKI Introduces Japan's First Iris Recognition for Camera-equipped Mobile Phones and PDAs.” 27 Nov 2006. Press Release.

[56] John Daugman, “Flat ROC Curves, Steep Predictive Quality Metrics: Response to NIST-7440 and FRVT/ICE2006 Reports” Unpublished manuscript. 2007.

[57] U.S. DHS. Coast Guard “Transportation Worker Identification Credential (TWIC) Implementation in the Maritime Sector; Final Rule” [Washington D.C.]: The Department, 25 Jan 2007.

[58] Authenti-Corp. “Draft final report: Iris recognition study 2006.” Technical report, v. 1.0, 1 Sep 2007.

[59] Viisage Technology. “Viisage to acquire leading iris recognition company SecuriMetrics, creating the industry’s only U.S.-based finger, face and iris multi-modal biometric offering,” 6 Feb 2006 Press Release.

[60] N. Gibbs, “Apocalypse Now.” *Time.com* 01 Jul 2002, [cited 6 Mar 2008], Available: http://www.time.com/time/magazine/article/0,9171,1002759,00.html.

[61] Ed Capizano, International Longshore and Warehouse Union Representative. Telephone interview. 31 Jan 2008.

THIS PAGE INTENTIONALLY LEFT BLANK

Response Summary for "Biometric Attitudes"

Total Started Survey: 99
Total Completed Survey: 74 (74.7%)

Show this Page Only

Page: Privacy Act and Informed Concent

1. I have read and understand that my participation in this survey is voluntary. And I consent to the above term.

	Response Percent	Response Count
YES- I Agree	100.0%	99
No	0.0%	0
answered question		99
skipped question		0

Show this Page Only

Page: Way Biometrics Might be Used

1. In your view, would the following scenarios be very acceptable, somewhat acceptable, not very acceptable, or not acceptable at all?

	Very Acceptable	Somewhat Acceptable	Not Very Acceptable	Not Acceptable At All	Don't Know	Response Count
Detectives could take a fingerprint found at a crime scene, turn it into a biometric reading, and use this to search state and federal databases of convicted offenders.	**90.8% (79)**	9.2% (8)	0.0% (0)	0.0% (0)	0.0% (0)	87
Police in patrol cars who stopped a driver for highway violations could take a computer scan of a driver's finger, and then use a computer terminal in the patrol car to check this against a database of fugitives involved in serious crimes	**59.8% (52)**	20.7% (18)	14.9% (13)	3.4% (3)	1.1% (1)	87
Law enforcement agencies could use finger or hand scan biometrics to allow only authorized officials to enter law enforcement intelligence files	**78.2% (68)**	18.4% (16)	1.1% (1)	1.1% (1)	1.1% (1)	87
Police could use facial recognition technology to scan the features of people attending major sports events						

or public ceremonies, looking for fugitives for serious crimes whose facial formulas they had in their system	**40.2% (35)**	24.1% (21)	18.4% (16)	14.9% (13)	2.3% (2)	87
Law enforcement agencies could create a biometric database of all persons convicted of a serious crime, for use in later criminal investigations.	**79.3% (69)**	18.4% (16)	2.3% (2)	0.0% (0)	0.0% (0)	87
					answered question	**87**
					skipped question	**12**

Show this Page Only

Page: Way Biometrics Might be Used - II

1. In your view, would the following scenarios be very acceptable, somewhat acceptable, not very acceptable, or not acceptable at all?

	Very Acceptable	Somewhat Acceptable	Not Very Acceptable	Not Acceptable At All	Don't Know	Response Count
School security guards could screen people entering a school, and compare the scans against a biometric database of convicted child molesters	**60.7% (51)**	22.6% (19)	6.0% (5)	8.3% (7)	2.4% (2)	84
To prevent people from obtaining double welfare benefits, officials could screen people seeking welfare checks against a biometric database of those eligible for the benefit.	**60.7% (51)**	28.6% (24)	2.4% (2)	4.8% (4)	3.6% (3)	84
Election officials could check a biometric database of convicted criminals and others who are not eligible to vote, and bar such persons from voting	**51.2% (43)**	28.6% (24)	10.7% (9)	8.3% (7)	1.2% (1)	84
Managers of high-security government facilities, such as laboratories or military bases, could screen people seeking entry against a biometric database of persons authorized to enter	**82.1% (69)**	14.3% (12)	1.2% (1)	1.2% (1)	1.2% (1)	84
Immigration officials could sign up persons wanting to speed up entry at passport-control stations, and process travelers more quickly in this way	**61.9% (52)**	27.4% (23)	3.6% (3)	4.8% (4)	2.4% (2)	84

answered question	84
skipped question	15

Show this Page Only

Page: Way Biometrics Might be Used - III

1. In your view, would the following scenarios be very acceptable, somewhat acceptable, not very acceptable, or not acceptable at all?

	Very Acceptable	Somewhat Acceptable	Not Very Acceptable	Not Acceptable At All	Don't Know	Response Count
Government agencies issuing required occupational licenses – such as for teachers, private guards, or nursing home workers – could check applicant's biometric against a database of criminal offenders not eligible to be licensed	**67.5% (54)**	21.3% (17)	7.5% (6)	2.5% (2)	1.3% (1)	80
Government agencies could use biometrics to screen individuals who seek access to "secure" rooms that are designed to all the processing of sensitive or classified information,to ensure they have been cleared to have such access	**82.5% (66)**	16.3% (13)	0.0% (0)	1.3% (1)	0.0% (0)	80
					answered question	80
					skipped question	19

Show this Page Only

Page: Way Biometrics Might be Used - IV

1. In your view, would the following scenarios be very acceptable, somewhat acceptable, not very acceptable, or not acceptable at all?

	Very Acceptable	Somewhat Acceptable	Not Very Acceptable	Not Acceptable At All	Don't Know	Response Count
Automated teller machines (ATM's) operated by banks could require a biometric for withdrawing funds in addition to your ATM card and PIN.	**37.2% (29)**	30.8% (24)	19.2% (15)	12.8% (10)	0.0% (0)	78
Automated teller machines (ATM's) operated by banks could require a biometric for withdrawing funds without an ATM card.	25.6% (20)	**34.6% (27)**	23.1% (18)	15.4% (12)	1.3% (1)	78

Computer system managers could use a biometric to admit persons authorized to access sensitive files, such as medical or financial information.	**47.4% (36)**	36.8% (28)	10.5% (8)	3.9% (3)	1.3% (1)	76
Gambling casinos could use facial scanning technology to screen out professional card counters or others banned from gambling in the casinos.	**32.1% (25)**	24.4% (19)	20.5% (16)	20.5% (16)	2.6% (2)	78
Employers could check the biometric of job applicants against a government database of convicted felons.	**48.7% (38)**	33.3% (26)	9.0% (7)	9.0% (7)	0.0% (0)	78
Stores selling guns could be required by check each person seeking to buy gun against a federal-government database of convicted felons and others not allowed by law to purchase firearms.	**70.1% (54)**	22.1% (17)	3.9% (3)	3.9% (3)	0.0% (0)	77
Credit card firms could offer card members a biometric to verify their identity for large transactions, and increase the security of credit card transactions.	**48.7% (38)**	30.8% (24)	9.0% (7)	10.3% (8)	1.3% (1)	78
					answered question	**78**
					skipped question	**21**

Show this Page Only

Page: Way Biometrics Might be Used - V

1. In your view, would the following scenarios be very acceptable, somewhat acceptable, not very acceptable, or not acceptable at all?

	Very Acceptable	Somewhat Acceptable	Not Very Acceptable	Not Acceptable At All	Don't Know	Response Count
Employers could use biometric scanners to note when employees enter or exit their facilities. For hourly employees, this system would function as a "time-clock." It would also improve employee safety: in the event of a fire or other disaster, the system could be used to immediately produce a list of all employees in a building.	29.5% (23)	**33.3% (26)**	19.2% (15)	17.9% (14)	0.0% (0)	78
Think of a store where you shop on a						

regular basis. The store has purchased an iris scanner that can scan you as you walk through the front door without the need for you to stop or face in a certain direction. Each time you enter that store your iris will be scanned so that the store can make note of your patronage. The store will use this information to alert employees of your presence (and pull up your recent purchases) so that they can provide you with personalized assistance. If you wish, you will be able to have the system automatically send coupons to your mobile phone as you enter as well.	7.7% (6)	12.8% (10)	23.1% (18)	**53.8% (42)**	2.6% (2)	78
					answered question	**78**
					skipped question	**21**

Show this Page Only

Page: General opinions of iris scanning.

1. Given this Scenario please answer the following questions. Please note the order of the choices, with Strongly Disagree to Strongly Agree from left to right.

	Strongly Disagree	Somewhat Disagree	Neither Agree or Disagree	Somewhat Agree	Strongly Agree	Response Count
I would be comfortable having my iris scanned to obtain a credit card.	**34.2% (26)**	18.4% (14)	14.5% (11)	23.7% (18)	9.2% (7)	76
I would be comfortable having my iris scanned to obtain a passport.	19.7% (15)	6.6% (5)	10.5% (8)	**35.5% (27)**	27.6% (21)	76
I would be comfortable having my iris scanned to obtain a driver's license.	25.0% (19)	15.8% (12)	11.8% (9)	**30.3% (23)**	17.1% (13)	76
I would be comfortable having my iris scanned to obtain a social security number.	25.0% (19)	6.6% (5)	9.2% (7)	**30.3% (23)**	28.9% (22)	76
I would be comfortable if hospitals gave newborns iris scans.	**38.2% (29)**	19.7% (15)	11.8% (9)	13.2% (10)	17.1% (13)	76
If the US government were to collect iris scan of everyone in the United States, I believe that the iris scan would only be used for official purposes such as confirming a person's identity at an airport.	**51.3% (39)**	18.4% (14)	7.9% (6)	15.8% (12)	6.6% (5)	76
					answered question	**76**

skipped question	23

Show this Page Only

Page: General Questions about Iris Technolgy

1. Please answer the following questions:

	Strongly Disagree	Somewhat Disagree	Neither Agree or Disagree	Somewhat Agree	Strongly Agree	Response Count
I think that iris scans are unique for each individual.	6.6% (5)	2.6% (2)	23.7% (18)	**35.5% (27)**	31.6% (24)	76
I think that the patterns on an iris can be duplicated well enough to fool a scanner.	10.5% (8)	9.2% (7)	**52.6% (40)**	22.4% (17)	5.3% (4)	76
I think that it will become so easy to duplicate an iris that, if iris scanners were widely used, iris prints would be stolen on a regular basis.	10.5% (8)	9.2% (7)	**48.7% (37)**	25.0% (19)	6.6% (5)	76
					answered question	76
					skipped question	23

2. Please answer the following questions:

	Strongly Disagree	Somewhat Disagree	Neither Agree or Disagree	Somewhat Agree	Strongly Agree	Response Count
Do you have any concerns of physical injury with the use of iris scanners	18.9% (14)	12.2% (9)	**33.8% (25)**	31.1% (23)	4.1% (3)	74
					answered question	74
					skipped question	25

Show this Page Only

Page: Safety Concerns about Iris Technolgy

1. Please answer the following question:

	Strongly Disagree	Somewhat Disagree	Neither Agree or Disagree	Somewhat Agree	Strongly Agree	Response Count
Knowing this, do you now have any concerns of physical injury?	**26.7% (20)**	18.7% (14)	**26.7% (20)**	25.3% (19)	2.7% (2)	75

answered question	76
skipped question	24

Show this Page Only

Page: Identity Theft

1. Some individuals fraudulently assume the identity of other persons in order to engage in illegal acts. To the best of your recollection, have you ever read or heard about people doing this in any of the following ways?

	Yes	No	Response Count
To apply for government welfare payments to which they were not entitled	**76.6% (59)**	23.4% (18)	77
To cash forged personal checks	**83.1% (64)**	16.9% (13)	77
To use stolen credit cards	**89.5% (68)**	10.5% (8)	76
To obtain a credit card in someone else's name	**85.7% (66)**	14.3% (11)	77
To obtain unauthorized access to confidential computer files	**66.2% (51)**	33.8% (26)	77
		answered question	**77**
		skipped question	**22**

2. How serious a problem do you think this sort of thing poses today?

	Very Serious	Somewhat Serious	Not Very Serious	Not Serious at All	Don't Know	Response Count
I would say this problem is :	**79.2% (61)**	19.5% (15)	1.3% (1)	0.0% (0)	0.0% (0)	77
					answered question	**77**
					skipped question	**22**

3. Have you ever been the victim of identity theft?

	Response Percent	Response Count
Yes	19.7%	15
No	**71.1%**	54

Don't Know	9.2%	7
answered question		**76**
skipped question		**23**

Show this Page Only

Page: More questions

1. How would you rate your political orientation.

	Politically Conservative	Somewhat Conservative	Middle-of-the-Road	Somewhat Liberal	Politically Liberal	Response Count
Please rate your political orientation:	25.7% (18)	**27.1% (19)**	25.7% (18)	15.7% (11)	5.7% (4)	70
answered question						**70**
skipped question						**29**

2. Have you even been the victim of a violent crime?

	Response Percent	Response Count
Yes	6.6%	5
No	**90.8%**	69
Don't Know	2.6%	2
answered question		**76**
skipped question		**23**

Show this Page Only

Page: Biometric experience in your life.

1. How often do you have your fingerprint scanned on a monthly basis.

	Response Count
view	72
answered question	**72**
skipped question	**27**

2. Some people oppose the use of finger-imaging biometrics to verify a person's identity, because they feel this procedure is like finger printing and seems to treat people like presumed criminals. Other people approvefinger-imaging identification as an easy-to-use process that helps protect individuals and the public against fraud. Which of these two views comes closest to your own?

	Response Percent	Response Count
Finger imaging treats people like presumed criminals	6.7%	5
Finger imaging helps protect individuals and the public against fraud	**81.3%**	61
DON'T KNOW	12.0%	9
answered question		**75**
skipped question		**24**

3. How often do you have your iris scanned on a monthly basis.

	Response Count
view	73
answered question	**73**
skipped question	**26**

4. Some people oppose the use of iris scanning biometrics to verify a person's identity, because they feel this procedure is similar to finger printing and seems to treat people like presumed criminals. Other people approve iris scanning identification as an easy-to-use process that helps protect individuals and the public against fraud. Which of these two views comes closest to your own?

	Response Percent	Response Count
Iris Scanning treats people like presumed criminals	8.0%	6
Iris Scanning helps protect individuals and the public against fraud	**64.0%**	48
DON'T KNOW	28.0%	21
answered question		**75**
skipped question		**24**

5. How often do you use voice recognition, which is based on the frequency patters in a persons voice, on a monthly basis.

	Response

	Count
view	73
answered question	**73**
skipped question	**26**

Show this Page Only

Page: Moral or Religious Concerns

1. Do you have any moral or religious concerns regarding the use of biometrics to help establish or verify your identity?

	Response Count
view	69
answered question	**69**
skipped question	**30**

Show this Page Only

Page: Demographics (*Optional)

1. What is your age:

	Response Count
view	73
answered question	**73**
skipped question	**26**

2. Please enter your gender:

	Response Percent	Response Count
Male	**54.7%**	41
Female	45.3%	34
answered question		**75**

	skipped question 24

3. What is the highest level of education you have achived?

Education Level

	Some High School	High School Graduate	Some College	Some Technical/Trade Traning	College Graduate	Technical or Trade School Graduate	Some Post Graduate Schhol	Masters Degree	PH. D.	Response Count
Education Level	0.0% (0)	0.0% (0)	14.9% (11)	1.4% (1)	**36.5% (27)**	1.4% (1)	24.3% (18)	18.9% (14)	2.7% (2)	74
									answered question	**74**
									skipped question	**25**

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California