NPS-CS-11-005

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

BIOMETRIC CHALLENGES FOR FUTURE DEPLOYMENTS: A STUDY OF THE IMPACT OF GEOGRAPHY, CLIMATE, CULTURE, AND SOCIAL CONDITIONS ON THE EFFECTIVE COLLECTION OF BIOMETRICS

by

Paul C. Clark, Heather S. Gregg, with preface by Cynthia E. Irvine

April 2011

This page is intentionally blank.

NAVAL POSTGRADUATE SCHOOL
Monterey, California 93943-5000

Daniel T. Oliver
President

Leonard A. Ferrari
Executive Vice President and
Provost

This report was prepared for John Grilli and funded by the United States Army G3 Biometrics Task Force.

This report was prepared by:

Paul C. Clark
Research Associate

Heather S. Gregg
Research Associate

Cynthia E. Irvine
Research Associate

Reviewed by:

Peter Denning
Chairman
Department of Computer Science

Released by:

Karl A. van Bibber, Ph.D.
Vice President and Dean of Research

This page is intentionally blank

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE ***(DD-MM-YYYY)***	**2. REPORT TYPE**	**3. DATES COVERED** ***(From - To)***
01-04-2011	Technical Report	Feb 2010 – Sep 2010

4. TITLE AND SUBTITLE
Biometric Challenges for Future Deployments: A Study of the Impact of Geography, Climate, Culture, and Social Conditions on Effective Collection of Biometrics

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Paul C. Clark, Heather Gregg and Cynthia Irvine

5d. PROJECT NUMBER
R61DH

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER
NPS-CS-11-005

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army G3 Biometrics Task Force
347 W. Main Street
Clarksburg, WV 26301

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

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

13. SUPPLEMENTARY NOTES
The view expressed in this report are those of the authors and do not reflect the official policy or position of the Department of Defense of the U.S. Government.

14. ABSTRACT
In February 2008 the Deputy Secretary of Defense signed a DoD Directive that established the Secretary of the Army as the DoD Executive Agent for DoD biometrics. The directive also indicated the importance of biometrics as a fully integrated enabling technology intended to support military operations. Even before that directive was signed, biometrics was being used extensively in a range of military operations. Despite its success, there has been little investigation of the potential use of biometrics in future operations. This report consists of two parts, which summarize the conditions under which biometric collection may occur in future Army deployments. Part I describes a range of biometric modalities and discusses technical factors associated with their use in various environmental contexts. Part II describes social and anthropological considerations that lead to effective biometric collection.

15. SUBJECT TERMS
biometrics, geography, climate, culture, social, collection

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			Paul C. Clark
Unclassified	Unclassified	Unclassified	UU	67	**19b. TELEPHONE NUMBER** ***(include area code)*** 831.656.2395

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

This page is intentionally blank

NAVAL POSTGRADUATE SCHOOL
CENTER FOR INFORMATION SYSTEMS SECURITY STUDIES AND RESEARCH

Biometric Challenges for Future Deployments

A Study of the Impact of Geography, Climate, Culture, and Social Conditions on the Effective Collection of Biometrics

Paul C. Clark, Heather S. Gregg, with preface by Cynthia E. Irvine

April 2011

This page is intentionally blank.

Preface

In February 2008 the Deputy Secretary of Defense, Gordon England, signed a DoD Directive [1] that established the Secretary of the Army as the DoD Executive Agent for DoD biometrics. The directive also indicated the importance of biometrics as a fully integrated enabling technology intended to support military operations.

Even before that directive was signed, biometrics was being used extensively in a range of military operations. Despite its success, there has been little investigation of the potential use of biometrics in future operations.

This report consists of two parts, which summarize the conditions under which biometric collection may occur in future Army deployments.

Factors affecting biometric collection include geography, climatic conditions, ethnic populations, and relationships with host countries. The attitudes of members of ethnic populations were considered to be a particularly challenging factor affecting biometric collection. In early work on this project a group of experts gathered for round-table discussions of the problem of biometric collection in diverse environments. Members of the group had diverse background, but many focused their research on the needs of special operations communities. Individual expertise ranged from the technical application of biometric modalities to the social and anthropological aspects of operations in limited warfare situations. Members of the group included both civilians and active military officers. These discussions lead to several observations.

First, the environmental context should be considered in the selection of an appropriate biometric modality. Part I of this report addresses technical considerations regarding the selection of modalities.

Second, social and anthropological considerations cannot be generalized even in relatively small regions. The group discussed several potential deployment areas and concluded that population demographics can be extremely diverse even in a single city. One example was Lagos, Nigeria. Due to political and economic factors, different regions of the city currently and in the future will support populations with widely different attitudes toward various biometric collection devices. Enclaves exhibiting relatively homogenous ethnic and religious characteristics are found throughout the city. How one approaches any one of these enclaves will depend upon long-term cultural factors as well as their exposure to modern technology. Some groups will find certain biometric modalities more acceptable than others, however these preferences are rapidly changing as new technologies are introduced. The combination of sometimes massive and rapid migrations of large groups of people coupled with rapid technological change thus make it difficult to predict the proclivities of a population in a particular area.

Third, technological change will affect biometric collection. Consider, for example the use of television. From the early 1900's through approximately 1941, television was exotic and largely confined to experimentation. Yet, by 1951 television networks could

be found across the United States. By 1985, color television was in virtually global use. However, television ownership per capita is still low in many parts of the third world with fewer than 100 televisions per 1000 people. The rise of cell phone use has been even more rapid and dramatic. Digital telephone networks were first available in the early 1990s. Now they are ubiquitous. Africa, in particular, is witnessing an extremely rapid rise in the use of wireless devices and cell phones. By 2004, mobile phone penetration in Africa was one phone per nine people and more than doubled by 2006. [2] Throughout Africa, cell phone penetration was estimated to be 30% by 2008. [3] As cell phones and other internet-based services become more integrated, multi-factor authentication techniques, including the use of biometrics, may become more prevalent. Thus, resistance to biometric collection may lessen as a result of familiarity with the use of biometrics for other purposes and populations that five years ago may have been averse to the use of biometric collection devices with cell phone-like form factors will now be much more receptive to the use of such instruments.

Part I describes a range of biometric modalities, discusses technical factors associated with their use in various environmental contexts. Assumptions that can serve as axioms in discussions of future uses of each modality are described. An analysis and recommendations regarding each modality is provided. Suggestions for future examination and research are provided on a per-modality basis. Table 4 of this part of the report summarizes recommendations for the use of modalities in various conditions. Overall recommendations for current and future biometric collection complete Part I.

Part II is an examination of factors that lead to effective biometric collection. Interviews were conducted with many individuals involved in the operational use of biometrics, many of whom had collected biometrics in theater, primarily in Iraq and Afghanistan. A surprising finding was that culture is not likely to be a major factor in biometric collection. The analysis led to several recommendations regarding the use of biometrics and provides a list of questions the answers to which can significantly affect the nature of a biometrics collection effort and its ultimate success.

References

[1] DoD Directive 8521.01E, Department of Defense Biometrics, 28 February 2008 http://www.dtic.mil/whs/directives/corres/pdf/852101p.pdf
[2] “Why Africa?”, Entrepreneurial Programming and Research on Mobiles, 2009. http://media.mit.edu/ventures/EPROM/whyafrica.html
[3] Africa Has 300 Million Mobile Phone Subscribers, International Telecommunications Union, 13 June 2008. http://www.itu.int/ITU-D/ict/newslog/Africa+Has+300+Million+Mobile+Phone+Subscribers.aspx

Part I
Contextual Considerations for Biometric Modality Selection

Paul C. Clark

This page is intentionally blank.

Part I
Table of Contents

Table of Tables

Table of Figures

1 Background

1.1 Definitions

When a biometric sample or trait is acquired, such as a picture of a fingerprint, the captured data goes through some amount of processing to prepare it for the extraction of a relatively small set of numbers, which represent the most unique aspects of the data. This extracted set of numbers is stored in a record called a *template*. A newly created template can either be *enrolled* into a system by adding it to a database of other templates, or it can be *compared* to previously enrolled templates. There are two basic usage scenarios for biometrics, known as *verification* and *identification*, which correlate to the breadth of a template comparison.

Verification is the scenario where a newly created template is compared with only one other template in a database, which is described as a one-to-one comparison. The classic example of verification is using biometrics to control physical access to a building, which requires a person to make a claim about who is attempting to gain access. The biometric sample is then offered as evidence of the claimed identity. In this example, the claimant submits to the acquisition of the sample, which gets transformed into a template, which is then compared against the enrolled template for the claimed identity.

The second biometric usage scenario is called *identification*, which is used when it is necessary to compare a newly created template to many enrolled templates, which is described as a one-to-many comparison. The classic example of identification is the use of biometrics in forensics, such as when a latent fingerprint is found at a crime scene. The investigator does not know who left the print, but the investigator wants to identify to whom it belongs. The latent fingerprint is transformed into a template, which is then compared against all the enrolled templates to determine if the person who left the fingerprint at the crime scene has been enrolled in the system, which may then link a name (and a face?) to a suspect.

A *modality* is a human physical or behavioral trait that can be used in a verification or identification scenario to recognize people. A common synonym for *modality* is *biometric*, but to avoid confusion between the plural of biometric (biometrics) and the "science of establishing the identity of an individual based on the physical, chemical or behavioral attributes of the person" [1] (i.e., biometrics), the term modality is the preferred term of art. When one modality is used by a system, then the system is referred to as a *uni-modal* system or a *mono-modal* system. When more than one modality is used in a system it is generically referred to as a *multi-modal* system, but the reference may be more specific, e.g., a system that uses two modalities may be referred to as *bi-modal.*

1.2 Assumptions and Limitations

As required, this report considers potential deployments over the next five, ten, and twenty years. For biometrics, the following assumptions are made with respect to technological advancements during these time increments.

Table 1 Assumptions of Technological Advances

Time Increments	Assumptions
2 years	There will be no significant technological advances that will be fielded by the DoD.
5 years	New statistical approaches will increase the accuracy of face recognition to very high levels in controlled environments (e.g., good lighting). [2] [3]
	The speed of face recognition will improve to allow it to be used effectively in identification scenarios with good quality images.
	A quality palmprint can be acquired by raising a hand in front of a camera, rather than placing it on a plate.
	Palm vein sensors will shrink in form factor to allow consideration in systems used in the field.
	The retina, as a biometric modality, will **not** re-emerge as a viable product. [4]
10 years	Within a lab environment, DNA processing and template creation time will shrink from hours to a few minutes. [5] [6] Palmprints can be taken with a camera at three to six feet.
20 years	Using portable devices, DNA processing and template creation time will be performed in the field. [7]
	The cost of DNA processing will be dramatically less.
	In addition to the growing number of fingerprints, the FBI database will include millions of iris and palmprint templates.
	Face recognition will work effectively in uncontrolled lighting conditions with cooperative users.

This study does not cover warehouse or transportation conditions for biometric equipment or its support equipment; the study focuses on operational conditions.

The following modalities were considered:

- Fingerprint
- Iris
- Palmprint
- Hand vein
- Voice
- Face
- DNA

The following modalities were explicitly excluded from consideration:

- Retina

Despite its accuracy, retina recognition is currently not a viable product. High costs, slow capture times, and user acceptance problems led to its demise. It is not likely to see a comeback.

- Hand Geometry
  Hand geometry does not offer enough uniqueness to be used with large populations without suffering from an unacceptably large false accept rate.
- Face Thermography
  Though thermography may be used as an approach for preventing some spoofing attacks with regular face recognition, by itself it suffers from too many environmental and permanence problems as a primary modality.
- Gait
  Despite continued interest and research, gait recognition is expected to suffer from large false accept rates and false reject rates, especially within a large population.
- Keystroke
  There are a few companies that sell keystroke-related products, but this modality currently suffers from high false reject rates due to the difficulty of capturing consistent information.
- Signature
  The market and interest in automated signature recognition was considered too small to include in this report. It currently suffers from high error rates. Its related modality, automated handwriting recognition, was also not considered in this report.

1.3 Modality Measurements

There is no straightforward answer to the question of which modality is the best overall because there are too many different ways modalities can be used, there is too much variability between potential user populations, there are too many potential environments in which a biometric system could be fielded, and there are too many potential design goals for a biometric system. However, there are some agreed upon measures of modalities [8] that help to narrow the possible choices for a potential system, as described below:

- ***Universality*** is a measure of the existence or usability of a modality within a population of interest.
- ***Distinctiveness*** is a measure of the uniqueness of a modality within a population of interest.
- ***Permanence*** is a measure of the stability of a modality over time.
- ***Collectability*** is a measure of the ease with which a sample for a modality may be acquired, which includes issues that may impede the acquisition and management of a good sample, such as environmental constraints, distance between users and the acquisition devices, template size, user awareness of the acquisition, and user convenience.
- ***Performance*** includes the accuracy of the modality and the speed with which comparisons can be made.
- ***Acceptability*** is a measure of the social approval of the modality for its intended use within the population of interest.

- ***Resistance to Circumvention (or Unspoofability)*** is a measure of a system's ability to defend detect or defend against any attempt to fool the system, either to impersonate someone during a verification, or to trick a system to declare a non-match during identification.

The first three measures are unchanging properties of a modality, while the last three measures are dynamic, based on current technology and social views, while the collectability category somewhat straddles those two distinctions. Not included in the measures listed above is the potential cost of a biometric system based on a given modality, though one may argue that it falls under the performance category.

Assigning a rating or score for each of the above measures for each modality is subjective and open to debate, especially if the target population is the entire population of the world. However, Table 2 is one attempt to do that for the modalities being considered for this report.

Table 2 Modality Comparison (Adapted from [8])
The rating system shows an 'H' for high, 'M' for medium, and 'L' for low. 'H' is the best possible rating.

Modality	Universality	Distinctiveness	Permanence	Collectability	Performance	Acceptability	Unspoofability
Fingerprint	M	H	H	M	H	M	M
Iris	H	H	H	M	H	L	H
Palmprint	M	H	H	M	H	M	M
Hand Vein	M	M	M	M	M	M	H
Voice	M	L	L	M	L	H	L
Face	H	L	M	H	L	H	L
DNA	H	H	H	L	H	L	L

The subjectivity of the ratings shown in Table 2 can be illustrated by noting that the universality of fingerprints is rated as medium, which is debatable. One can surmise that the reason for the medium rating is based on the fact that a large majority of the world's population still performs manual labor to make a living, which tends to wear off fingerprints to the point that many of today's sensors cannot obtain an acceptable acquisition.

All the measurements described above are important for this report. However, for this report it is necessary to break down the collectability measurement into the following operational conditions:

- Temperature (hot/cold)

- Humidity (dry/wet)
- Dusty and Sandy

Table 3 provides the operating conditions and terminology associated with the weather that this report considers.

Table 3 Climatic Conditions (Adapted from [9])
The designations in parentheses under the Daily Cycle *refer to climatic categories.*

Climatic Design Type	Daily Cycle	Operational Conditions		
		Ambient Air Temperature (°F)		Ambient Relative Humidity
		Daily Low	Daily High	
Hot	Hot Dry (A1)	90	120	8 to 3
	Hot Humid (B3)	88	105	88 to 59
Basic	Constant High Humidity (B1)	Nearly Constant 75		95 to 100
	Variable High Humidity (B2)	78	95	100 to 74
	Basic Hot (A2)	86	110	44 to 14
	Intermediate (A3)	82	102	78 to 43
	Basic Cold (C1)	-25	-5	Tending toward saturation
Cold	Cold (C2)	-50	-35	Tending toward saturation
Severe Cold	Severe Cold (C3)	-60		Tending toward saturation

See Appendix A for a map that associates the climatic design types shown in Table 3 to the various regions of the world.

2 Environmental Issues Affecting Modalities

In this section each of the identified environmental issues shall be discussed with respect to each modality of interest. In 2007, the Defense Science Board (DSD) made the following recommendation:

> Given the expected expansion of biometrics applications and use-case scenarios, ensure that field-use biometrics collection and analysis systems are designed to function effectively across the whole range of physical environments. If there are cases where the basic science involved prohibits or inhibits this, identify and document these for the benefit of operational planners. [10]

It is expected that this report will help the DoD to meet the above recommendations.

2.1 Temperature

2.1.1 Cold Temperatures

"The areas designated as cold, and severe cold, primarily northern North America, Greenland, northern Asia, and the Tibetan Highlands of China, were delimited because of the occurrence of low temperatures." [9] See Appendix B for the minimum temperatures associated with the various regions of the world.

Generally, any biometric sample acquisition device that requires the exposure of skin is risking operational issues in cold and severe cold environments, which includes the operator of the device and the subjects of interest. Frostbite becomes a real risk at -13° F. [11] In colder fielded environments the acquisition device will need to be designed in such a way that a heavily gloved operator will be able to manage an acquisition session with one or more subjects. Enrollment would require skin exposure, which would not bode well in either a cooperative or uncooperative population. Skin must typically be exposed for enrollment with the following modalities of interest: fingerprint, palmprint, hand vein and face.

The collection devices need to be built to withstand long exposures to cold temperatures. Batteries are a specific concern for portable collection devices, which was an issue in Afghanistan. [12] Batteries operate effectively within a given temperature range, but they dissipate a charge much quicker in cold temperatures. [13] In addition, cycling between warm and cold temperatures reduces the lifespan of a battery. [13] The logistical effect that batteries have in cold environments, when compared to normal environments, is that troops would need to carry more batteries to perform a similar biometric acquisition task, and they would need to have more replacement batteries at their disposal. These problems can potentially be overcome by using battery technology that is less affected by cold temperatures (if they exist), or by other means to keep the batteries warmer than the environment.

It has been assumed that cold fingers affect the quality of a fingerprint acquisition because a good-quality print requires pliable skin, which may not be the case if fingers

are cold and stiff. However, a recent Canadian study shows little correlation between temperature and fingerprint acquisition quality [14]; additional research is needed to verify the results. The same study indicated that the use of a fingerprint sensor for verification in a cold environment "had a good level of usability," and that removing "gloves to use the sensor was reported to be roughly equivalent to the use of [car] keys," which is assumed to mean the bare-skinned retrieval and use of car keys. Even though the verification occurred outdoors in this research, it should be pointed out that the enrollment session was performed indoors with cooperative users.

The study of fingerprints in cold weather also examined the performance of optical and solid-state fingerprint sensors in cold weather. The results show that two capacitive sensors failed in basic cold weather, with one of the failures attributed to condensation. The optical sensors did not fail, but condensation under the platen did cause some matching errors. [14] If this result is verified as a result of additional research, then it presents a problem for portable devices because the solid-state sensors can achieve a smaller footprint within acquisition devices than the optical sensors. Unfortunately, the study did not include the newer sensors based on ultrasound, so additional research is necessary to make conclusions about which sensor type is best for colder weather.

With regard to forensics and the use of latent prints (finger or palm), cold temperatures may have an impact. Cold skin closes some pores, which means that less material will get transferred from the skin to a surface, which will cause poor quality latent prints. On the other hand, when the temperature of the receiving surface is cold, then the material left on a surface will stay longer than when it is warm. [15] There is an advantage, therefore, in cold weather if a latent print is deposited on a surface in a warm environment but the touched item is left outside in the cold.

For face recognition, there is the difficulty of the lens fogging up or forming condensation if the camera is moving between a cold outside environment to a warm indoor environment. When that kind of temperature change happens to a camera it may take a while for the condensation to evaporate before a picture may be taken. If the camera is taken back and forth between the two temperature environments within a short period of time, it causes the condensation to freeze and may potentially damage the camera. [16] One solution is to keep the camera at a stable temperature (e.g., with an internal heater), but that would reduce the time that a battery can hold a charge. Additional research is required in this area.

There appears to be no data on how cold weather affects voice recognition, but cold weather tends to make a voice shake, which would lead to a hypothesis that the accuracy of voice recognition is affected by cold weather. Research is required to verify that hypothesis.

Modalities that focus on vein patterns under the skin potentially suffer performance degradation due to cold weather because blood vessels constrict in such environments, changing their pattern [17] and making them less visible to the sensor. [18] Research is needed to determine the extent of the degradation.

Cold weather is beneficial when it comes to the handling of DNA samples because the ideal storage temperature in a lab is -4° F, while long-term storage temperatures may go as low as -94° F. [19]

The iris is reported to be unaffected by cold weather. [20]

Recommendations for Cold Weather Environments:

In summary, cold weather is a harsh environment that negatively affects the use of biometrics in many ways, whether because of a problem with the modality itself, or because of constraints on the current acquisition devices, or both. The following actions are recommended to prepare the DoD for actions in cold and severe cold weather:

1. Keep close track of the advancements in battery technology, or fund research into battery technology that can better withstand the effects of cold weather.
2. Research how cold weather affects the various kinds of fingerprint and palmprint sensors. Which sensor type operates best under cold conditions, or conversely, which sensor type fails in unacceptable ways?
3. Research how cold weather affects the quality of an acquired fingerprint.
4. Research how biometric enrollment can be facilitated in cold and very cold weather without causing major discomfort or injury to the collector and the collectees.
5. Research ways to use or build a camera that will not have condensation problems in the cold and very cold weather.
6. Research how cold weather affects voice recognition.
7. Research how cold weather affects finger vein and hand vein acquisition.

2.1.2 Hot Temperatures

"The areas where hot conditions apply include most of the low latitude deserts of the world. During summer in these areas, temperatures above 43°C (110°F) occur frequently, but except for a few specific localities, temperatures will seldom be above 49°C (120°F)." [9]

"Hot-dry conditions are found seasonally in the deserts of northern Africa, the Middle East, Pakistan, and India, southwestern United States, north central Australia, and northern Mexico." [9] See Appendix C for the maximum temperatures associated with the various regions of the world.

One study included the outdoor use of biometrics during summer months. The study used optical and solid-state sensors to acquire the fingerprint images. The solid-state sensor got "unbearably hot to touch". [14] However, this study had a fixed installation outside a door for access control, but it does point out that a device with solid-state sensors should have a requirement for a cover to shield it from prolonged direct sunlight. The same can be said for any sensor that requires human touch to complete the acquisition. The Marine Corps has reported that some biometric equipment suffered breakdowns in the heat because they were not ruggedized for extreme temperatures. [21]

On a related note, sources reported that operators had trouble with portable iris scanners and face cameras in bright sunlight [21][22], which is not necessarily exclusive to warm conditions, e.g., bright light reflected off of snow.

As mentioned in Section 2.1.1, cold weather is helpful for the storage of DNA samples, but that is not always true for hot weather. On one hand, a dry heat will dry out moist samples, which is desirable prior to packaging, but long-term exposure to hot temperatures will cause the DNA to degrade, which will negatively impact DNA analysis. If specially treated paper is used to collect samples (e.g., dropping blood onto it), then the paper can be stored at room temperature in dry environments. Otherwise, after moist samples are dried, they need to be quickly sent to a lab where they can be refrigerated or frozen. Long-term freezing of samples may be necessary if they are potentially going to be used as evidence in court, so such samples should be stored in a place where backup power is readily available. [19][23]

With respect to latent fingerprints, a hot surface can cause the print residue to either flow into an unidentifiable mess, or dry out completely, depending on the extremity of temperature. [15]

Recommendations for Hot Weather Environments:

1. Specify the ruggedization of biometric equipment to handle extreme heat.
2. Specify that biometric equipment must have interfaces that can be used in bright light.
3. Ensure that the handling of DNA samples in warm weather environments does not undermine the integrity of the samples.

2.2 Dust and Sand

Dust, which consists of particles smaller than sand, is not the same everywhere in the world. "In arid regions, soluble salts are common components of dust…In some regions, the dust-related problems with equipment such as fouling, interference of moving parts, increased electrical conductivity, and corrosion can be more pronounced if there are more reactive constituents in the natural dust." [9] Because of the small size of dust, it can get into very small openings of equipment. Common consequences of dust, depending on its composition, are seizing and sticking of moving parts, corrosion, and electrical problems. "Major regions where dust originates are the Sahara, the southern coast of the Mediterranean Sea, the northeast Sudan, the Arabian Peninsula, the lower Volga and North Caucasus in the former USSR, the pampas of Argentina, Afghanistan, and the western Great Plains of the US." [9] The Tarim Basin in China has dust storms from 25% to 50% of the year. However, the most common cause of airborne dust is moving vehicles over unpaved roads and other forms of mechanization, such as helicopters. Biometric equipment that will be used in the field should therefore be built to withstand dusty environments. The Marine Corps has reported that some biometric equipment suffered breakdowns in sandy conditions because they were not sufficiently ruggedized. [21]

Blowing sand in a dry environment can cause a buildup of electrostatic energy, which can cause shorts in sensitive electrical devices. Because of the larger particles, blowing sand may not get into small openings of devices like dust can, but sand can be very abrasive to exposed items, especially scratchable items such as the glass of a camera lens or the plate of a fingerprint sensor.

Dirty conditions can make it difficult to get a good acquisition of some modalities. The valleys between fingerprint ridges can get filled in with dirt, making it difficult to distinguish ridges and their minutiae when used with many kinds of sensor.

In a dusty environment (i.e., dust swirling in the air), people will protect their eyes by squinting, or covering their eyes with goggles, neither of which are conducive to iris or face recognition. In addition, breathing the dust is prevented with something covering the mouth, which will cause problems with face recognition and voice recognition.

Latent fingerprints can be affected by dust and sand, minimally covering them from view.

Recommendations for Dusty and Sandy Environments:

1. Specify the ruggedization of biometric equipment to handle dusty and sandy environments.
2. Establish procedures for collecting biometric data in dusty and sandy environments, if they do not already exist.

2.3 Humidity

The following quotes about humidity all come from [9]:

> "Warm, humid conditions can occur year-round in tropical areas, [and] seasonally in mid-latitude areas…. Other high levels of humidity can exist worldwide."
>
> "Since the amount of water vapor the air can hold increases with temperature, areas with the highest absolute humidities are hot locations (usually at the edge of a desert) adjacent to very warm bodies of water…The highest accepted dew point observation is 34°C (93°F), (100 percent [relative humidity] and 93.2°F) recorded in July (exact date unknown) at Sharjah, Arabia, on the shore of the Persian Gulf."

In highly humid environments DNA samples need to be collected quickly from a crime scene because the DNA molecules degrade quicker in such environments than in other environments, and because rain or mist will wash the cells away before they are collected. For moist DNA samples, such as blood, plastic bags are discouraged as a storage mechanism because they foster condensation, which mimics humid conditions and fosters mold. [19] To avoid the condensation problem, moist samples are supposed to be air-dried prior to packaging. All samples should be sealed in paper-based containers and stored in a dry environment. [19] If DNA samples are taken as part of an indoor registration then humidity is not as problematic, but outdoor collection in the field requires proper equipment and training to raise the likelihood that the samples to be of

worth when they get to the lab. When in-the-field DNA processing can take place in the future, then this handling problem will be mitigated.

In highly humid environments latent fingerprints degrade quickly on porous surfaces. Therefore, like DNA in such environments, latent fingerprints need to be lifted soon after a crime has been committed. [24] Cold and dry environments are preferable for the storage of DNA.

In wet environments fingers can become saturated and wrinkled, like when someone has been swimming for a while. In such situations it may not be possible to get a good acquisition of a fingerprint, resulting in reports of degraded accuracy. [25]

If the humidity is high enough to cause wet, saturated fingers on the subjects being enrolled (i.e., it is raining), then the fingers will need to be dried before acquisitions will be acceptable. This is problematic in hectic situations where speed is important, such as a raid in hostile territory. Highly humid environments can cause problems with equipment, as described elsewhere. [9]

On the other hand, dry air causes the skin to become dry, which is a problem for palmprints and fingerprints because dry, non-pliable skin does not lay flat on a sensor, causing the ridges to not have contact with the sensor, which causes the resulting fingerprint to be of poor quality. A poor quality print cannot be enrolled, and it will lead to false rejects for those already enrolled. This situation is usually dealt with by applying wet wipes or other lotions to the desired area of acquisition.

Moderate to heavy rain causes background noise, which can disrupt an attempt to obtain a good voice sample in the field. In addition, a wet microphone can potentially be damaged, and sounds recorded with a wet microphone are likely to be affected.

Rain causes problems when trying to acquire images of irises and faces in the field.

Recommendations for Humid Environments:

1. Establish procedures and potentially research ways to collect and handle DNA samples in very humid environments.
2. Research the effect of wet weather on the collection of fingerprint data and the best technologies and procedures for dealing with wet hands.
3. Specify the ruggedization of biometric equipment to deal with humidity.

3 Other Modality-Specific Issues

3.1 Fingerprint

The age of a subject has some interesting effects on the potential accuracy of a biometric system; depending on the modality it may help or hurt. Studies have shown that fingerprints of older subjects have a significant adverse effect on the quality of a fingerprint acquisition, which in turn has an adverse effect on the accuracy of matching decisions. [26] [27] [28] One study shows the degradation as linear over time [28], while

another reports a significant degradation for those over the age of 62 [29]. On the other end of the spectrum, fingerprints can be very difficult or impossible to enroll for children under the age of six, due to cooperation problems and fingerprint quality problems. [28] Newer ultrasound sensors could potentially remove the technical problems, but not the challenges of interacting with a frightened or otherwise uncooperative child.

The better-known problem with fingerprint permanence is the impact that manual labor has on the ability to acquire a usable fingerprint. [30] Bricklayers are the common example, where years of working with the rough surface of bricks wear the fingerprints to the point that they are not visible with optical or solid-state sensors. Even though the percentage of bricklayers in the world population is miniscule, there is a very large percentage of the population that still work with their hands to make a living, including children. The problem in Afghanistan was scarred and calloused fingers from harvesting poppies, a common cash crop in Afghanistan. [12] It is reasonable to hypothesize that the ultrasound fingerprint sensors can overcome the problems of worn fingerprints, but there is no mention of this benefit in the literature.

It has also been shown that women have a significantly higher quality in their fingerprint acquisitions when compared to men, though it appears that more studies need to be performed to better understand this phenomenon. [31]

Circumvention of a fingerprint-based system should be a concern. The motivation for circumvention can be either hiding one's identity or to be identified as someone else who has more privileges. Circumvention is usually accomplished when the system does not detect the *liveness* of the artifact presented to the sensor, such as a gelatin finger. Optical sensors are most susceptible to circumvention, which can be accomplished with a latex copy of a fingerprint glued to a fingertip. [32] Solid-state sensors are more difficult to circumvent, but they fail more often and sense an unacceptably smaller area of the fingertip. Ultrasound sensors are extremely difficult to circumvent but are very expensive. One approach to defend against the possibility of circumvention is to use one or more additional modalities, which the DoD already collects and employs.

With respect to automated recognition, there appears to be a DoD requirement or operational clash between fingerprints and irises. Fingerprints have many advantages over irises. The obvious forensic advantage is that the enemy often leaves latent prints, such as on IEDs, whereas there is no such thing as a latent iris print. Fingerprints can be used to identify a corpse, which cannot be done with the iris. Many potential host countries have criminal fingerprint databases that can be scanned into the DoD database. Such advantages tend toward forensics. However, for those who operate the fielded biometric systems that are used to interact with people, they prefer working with the iris. [33] Both sides of the operational use of biometrics could come to closer agreement if the time it takes to obtain a quality capture of an enrollee's fingerprints can be reduced, which can currently take several minutes. This is important because the strong operator preference toward the iris has led to lower-quality fingerprints and facial photos. [33]

Recommendations for Fingerprints:

In addition to the recommendations given in Section 2, the following are additional recommendations for fingerprints:

1. Perform research with ultrasound fingerprint sensors. How do they perform in the various environments and with poor quality fingerprints? Are they bulky and heavy? Is the quality of the resulting print acceptable? How long does it take to obtain a sample? Do they overcome problems related to older subjects? Do the benefits outweigh the costs?
2. Perform research with three-dimensional fingerprint sensors that are just now being developed. [34][35] How do they perform in the various environments and with poor quality fingerprints? Are they bulky and heavy? Is the quality of the resulting print acceptable? How long does it take to obtain a sample? Do they overcome problems related to older subjects?
3. Get involved with the research being done by NIST, sponsored by the Department of Justice, to create a "fast tenprint capture device". [36] The intent is to create a device that can quickly capture all five prints of a hand at once with the same quality and surface area of a rolled-ink print. Such a device would drastically reduce enrollment time and still be compatible with the FBI.
4. Perform additional research to determine whether gender truly does have an impact on fingerprint quality. If so, how can that fact be used to the advantage of the DoD? Or, what can be done to equalize the quality across gender?

3.2 Iris

It has been assumed that the iris has a high level of permanence, even after cataract surgery. [37] However, there is some anecdotal evidence [38] and initial studies [39][40] that contradict this permanence assumption, where one study shows 3%-4% degradation in matching scores over a four-year period. There is no database of iris images documenting the differences over a greater period, so it would be beneficial to study this phenomenon and provide concrete analyses to determine whether the results are a fluke, or whether there indeed is degradation, and whether it is linear over time or it plateaus. It has also been recommended to the FBI to perform such a study over ten years [38]. The following question needs to be answered: how much time may elapse between two iris captures of the same person before a system will conclude that they do not match? The results of this study can have a major impact on the operational use of the iris for verification and identification, as well as the periodicity of updates to collected iris data.

Iris recognition requires more cooperation from the targeted subject than when acquiring a fingerprint. If a subject does not want to cooperate with an iris acquisition, then it is very difficult to force the issue. Therefore, problems have been reported when the population included children, especially those under the age of four. [41]

There is a difference of opinion concerning the impact that very dark eyes have on the ability to enroll an iris. Near infrared (NIR) light is purposely used to bring out the rich iris patterns that exist with dark eyes, which are not usually discernable with visible light. Iris experts therefore claim that dark eyes have no negative impact (e.g., [42]**),** while others report anecdotal difficulties when eyes are darker than usual (e.g., [41]). A NIST presentation showed that the effect of dark eyes (vs. light eyes) is dependent on the

implementation, where one implementation showed lower quality captures with dark eyes, while with another implementation showed higher quality captures with dark eyes. [43] More research needs to be performed in this area to make conclusive recommendations, especially considering the vast populations in East Asian countries that have dark eyes.

When capturing an iris image for a particular person, each time an image is captured in the future, the amount of pupil dilation will be different, depending on the amount of light in the environment. Iris matching algorithms take this into account, but it has been shown that extreme differences between pupil dilation in the enrolled image and later captures will cause the system to falsely declare that they do not match. [44] The environment where iris collection takes place affects pupil dilation, such as an outdoor collection on a bright sunny day, or an indoor collection in a shady tent. For example, an overly bright day could cause a tight constriction of the pupil, which could potentially cause erroneous matching results. The capturing of iris images should therefore have procedural and technical controls to ensure an acceptable range of pupil size.

Recommendations for Irises:

In addition to the recommendations that may have been given in Section 2, the following are additional recommendations for irises:

1. If the FBI has not followed up on recommendations to study the permanence of iris patterns, then the DoD should get involved to scientifically study this open question.
2. Perform research to determine, once and for all, the affect that very dark eyes have on the quality of an acquired iris pattern, if any.
3. Establish procedural or technical controls to ensure that iris acquisitions do not include unacceptable pupil dilation or constriction, if such controls do not already exist.

3.3 Palmprint

Because of the size of an adult hand, traditional acquisition devices for hand geometry systems have been large, and therefore are not suitable for in-the-field acquisitions. However, research is being performed to allow for an easier acquisition using just a camera, such as having the enrollee raise a hand. [45] This has the potential advantage of allowing a simultaneous acquisition of a face and a hand. Because the distinctiveness of hand geometry is low, it should not be used on a large population, but the concept should be applicable to palmprint acquisition, assuming the use of a very high-resolution camera. Research should be performed in this area.

Palmprints are essentially a very large fingerprint and therefore roughly have the same advantages and disadvantages as fingerprints. However, palmprints have the added advantage of being even more discriminating than fingerprints, but at the cost of significantly larger templates.

Recommendations for Palmprints:

In addition to the recommendations that may have been given in Section 2, the following are additional recommendations for palmprints:

1. Perform research to determine how much resolution and/or telephoto capability is required for a camera to capture the fine detail of a palmprint at three to six feet.
2. Because the FBI will start including palmprints in its biometric database, the DoD should study the potential impact of adding palmprints to its database. The FBI justification for adding palmprints is that 30% of all crime scenes have latent palmprints. [46]

3.4 Hand Vein

Hand vein technology is a relatively new modality, which should be separated into *palm vein recognition* and *back of the hand vein recognition.* The approach with the back of the hand is not considered a viable alternative in this report. The palm vein approach has the advantage of being contact-less, and its accuracy has been compared to that of irises. [47] Unfortunately, the palm vein sensors are currently expensive and do not come in a small form factor, though this report predicts that the form factor will shrink in the future to allow them to be used in handheld devices in the field.

Recommendations for Palm Veins:

In addition to the recommendations that may have been given in Section 2, the following are additional recommendations for palm veins:

1. Perform research into palm vein technology to ensure it is technically feasible in the kinds of conditions the DoD is expected to encounter, and to verify the claims of accuracy.
2. Perform research to determine how the technology fares in the various environments considered in this report.

3.5 Voice

The voice continues to change from birth until the late teens, whereupon it will not change much unless damaged in some fashion, such as with extensive cigarette smoking, surgery on the vocal tract, or extensive yelling. [48] This modality should therefore only be used with adults, but with the understanding that aging still changes the voice.

Voice recognition does not work well in uncontrolled environments because of the high potential for background noises, which co-mingles with the sampled voice of interest, making it difficult for a voice recognition system to make good comparison decisions.

The great advantage of voice recognition is that it can be used to recognize someone over a great distance, such as via a telephone. Voice recognition can be done cooperatively to verify someone to a bank application, or it can be used to identify someone during phone wire-tapping.

The great disadvantage of voice recognition for identification is that a voice can be purposely changed if one knows that an enrollment is being performed for later forensic use, or changed when a sample is being taken during a raid so it will not match a previous enrollment. Therefore, voice recognition in the field appears to be limited to covert

usage, such as trying to link the voice in a video to voice prints in previous videos, messages, or other sources.

Recommendations for Voice:
In addition to the recommendations that may have been given in Section 2, the following are additional recommendations for voice recognition:

1. Continue to fund research into voice recognition algorithms to push the accuracy and utility of the technology.

3.6 Face

People from one race generally have a difficult time differentiating between large numbers of people in another race, which is known as the *other-race effect*. [49] Other-race effect has also been seen in automated face recognition systems. [50] Today's face recognition systems are developed after applying complex statistical evaluations on a large number of normalized facial images, which are referred to as the *training set.* If a training set has a bias toward a particular race, then problems may occur when people from another race interact with the system. For example, if a system's training set only consists of Caucasian faces then it will perform as designed if enrollees are all Caucasians. If one enrollee is non-Caucasian, then the system will have no difficulty with its matching decisions. However, if there are many non-Caucasian enrollees in this example system, then system accuracy will degrade. Therefore, if automated face recognition may potentially be used with all races, then the training set must represent that usage, and testing should be performed to ensure that accuracy is acceptable. If facial images are stored to allow a human to confirm a correct identification has been made based on other criteria, such as a fingerprint, then the other-race effect needs to be considered as part of the hiring qualifications and training program for the system operators.

Face recognition is the classic permanence problem because human faces age over time. Research into the effects of aging on automated face recognition accuracy has historically been challenging because of the expense and time it takes to compile a working set of images of people that were taken years apart, but there are now at least three publicly available databases. [51] [52] [53] Using images that were taken one year apart, one study showed that even such a small temporal difference caused degradation in performance. [54] However, it has been shown that older people are easier to recognize than younger people. [55] Using the available databases, additional studies need to be performed to consider the effects of aging on face recognition accuracy. There is a lot of research being conducted to either determine a person's age from a face image, or adjust the age of an image. [56]

Of particular interest may be the difficulty of enrolling and comparing faces of children under the age of a young teenager, which is another area that requires more research. The degradation in accuracy of automated face recognition due to aging of children is likely to be non-linear, such that the false reject rates would be significant. This is a DoD concern for automated face recognition if the people who need to be enrolled and automatically matched are under the age of fourteen (e.g., child terrorists). In addition to

the technical issues associated with enrolling children's faces, there are the problems related to uncooperative children who need to hold still and look straight into a camera.

One study reported enrollment problems when participants were wearing hats [57], though no details are given for the kind of hat to indicate whether it was causing shadows on important features, such as might occur with a baseball hat, or whether the face recognition was dependent on head shape, which was occluded by the hat. When it comes to passport photographs, the U.S. Department of State requires that no hats be worn or headgear that "obscures the hair or hairline". [58] One database of face images has images of people with and without scarves over their mouth. [59] Additional studies should be performed to consider how the different head coverings that might be seen around the world affect face recognition. Current standards permit a head covering if it is used for religious purposes only, and the standards do not allow the face to be covered at all [60], i.e., scarves that only reveal the eyes are not allowed because they obviously prevent face recognition. Facial hair has been reported to have no impact on enrollment or matching accuracy, [28] though it is not clear whether that is dependent on the presence of facial hair during enrollment and later acquisitions.

The available illumination during enrollment and later acquisitions has historically been an indicator of potential accuracy. One study found that the quality of illumination during enrollment was a better indicator of matching accuracy than the quality of illumination during verification. [57] Therefore, there has been a lot of research to develop a face recognition system that can be used in less-controlled environments, i.e., outdoors, that is not as dependent on a constant level of illumination. Such research includes the use of near infrared light (NIR) and NIR light sensors to acquire face images (e.g., [61]), as well as new approaches that continue to use visible light (e.g. [62][63]). However, illumination will continue to be a problem for many years for automated face recognition in outdoor situations. Therefore, current standards for face acquisitions require equally distributed lighting across the face, no shadows on the face (particularly the eye sockets), and conversely no bright spots on any part of the face. [60]

It is not uncommon in some cultures to tattoo part of the face, e.g., the Maori [64], while other cultures may practice extremes in piercings of the face other than the ears, i.e., eyebrows, nose and lip. It has been stated that tattoos and piercings can degrade face recognition accuracy [65], which is assumed to mean that the enrolled face image did not have such items, such that avoiding identification may be possible by applying them. If the DoD will need to use automated face recognition within cultures that commonly apply face tattoos and piercings, then studies should be performed to determine the impact that such practices have on the accuracy of face recognition. Studies may also be performed to consider ways to negate the potential spoofing aspects of face tattoos and piercings.

Because it has been determined that automated face recognition has higher recognition rates for men than for women, and higher recognition rates for older people than younger people [55], then there should be some concern if the population of interest is predominantly young women.

It has been shown that aging is accelerated with heavy cigarette smoking, excessive drinking of alcohol, and heavy drug use. [53] Populations with large concentrations of one of more of these tendencies may have higher false reject rates with respect to automated face recognition.

Recommendations for Face:
In addition to the recommendations that may have been given in Section 2, the following are additional recommendations for face recognition:

1. For any face recognition system under consideration by the DoD, require that it perform equally well with any race.
2. To facilitate research into face recognitions systems that work will all races, ensure that there exists a database of face images that reflect all races.
3. When training people to visually recognize someone from a photograph, make sure that training includes information about other-race effect.
4. Perform research into improving the accuracy of face recognition for templates created several years apart.
5. Perform research into how face recognition is affected by the traditional head coverings that are seen around the world.
6. Determine those nationalities or religions that will not remove a head covering for biometric enrollment.
7. Determine those nationalities or religions that will not remove a face covering, such as a scarf, for biometric enrollment.
8. Perform research to determine how face recognition is affected by facial hair if the amount of hair changes between enrollment and later acquisition (e.g., a beard during enrollment but shaved later).
9. Perform research that will improve the accuracy of face recognition in uncontrolled environments (e.g., poor lighting).
10. Perform research to determine the likelihood of interacting with cultures that heavily tattoo or pierce the face. If the likelihood is high, and the numbers are great, then it would be proactive to perform research into the effects that such practices have on the accuracy of automated face recognition.
11. Studies should be performed to determine the effectiveness of using tattoos (or face paint) and piercings to avoid identification, and to consider technical and non-technical approaches to deal with the problem.

3.7 DNA

Because of the time it takes to acquire and process a DNA sample, which is currently measured in hours at best [66], DNA is only used for identification scenarios, such as when determining a suspect for a crime and when faced with an unknown corpse. The DoD already has an Armed Forces DNA Identification Laboratory (AFDIL) that, among other responsibilities, stores DNA data on U.S. military members, which is used to identify U.S. personnel who are killed in combat. In addition to the AFDIL, the DoD collects DNA samples for forensic purposes from people in occupied areas and stores them in its Automated Biometric Identification System (ABIS). [67]

It does not take long to obtain a sample from a local resident in an occupied area, but currently the sample must be handled carefully so that samples are correctly marked. This is problematic because of the number of people who must handle and transport the sample between the acquisition and the data entry into a computer. This can be a problem if troops will be required to collect DNA samples in the field under stressful conditions. However, once DNA processing can be done within minutes (or less) in the field [7], and then transmitted to a central repository, this concern will have been minimized. However, this ability will not become a reality for about twenty years.

A recent paper from the RAND Corporation [68] openly questions the DoD's use of DNA from a monetary point of view, concluding that the DoD needs to evaluate whether the money spent on the DNA effort in Afghanistan and Iraq could be better spent on other activities. The DoD needs to respond to the issues raised in the paper.

Recommendations for DNA:
In addition to the recommendations that may have been given in Section 2, the following are additional recommendations for DNA:

1. In the future, if DNA processing is reduced to a few minutes in the field, then thought should be given to how this will change the handling of potential evidence in a court of law because DNA is especially prone to tampering.
2. Respond to the issues raised in the cited RAND report.

4 Other Technical Issues

There are several different biometric systems being used by the DoD that do not interoperate well, which cause additional processing delays as software attempts to translate the different formats to accommodate the differences. [69] In addition to the inter-DoD interoperability issues, there are non-DoD biometric systems.

Bandwidth and system response are problems for many applications, not just biometrics, but to be complete it is mentioned here. After capturing biometrics on detainees, it could take five hours to get a response whether they were wanted or not. [70]

It currently takes too much time to enroll someone. With inexperienced operators it can take 20 minutes per person for a full enrollment, which constitutes all ten fingerprints, five photos, both irises, and biographical information. Experienced operators perform a full enrollment in five-to-ten minutes. [12][22] This may be acceptable when enrolling detainees or cooperative locals within a host country, but it is probably unacceptable in other situations, such as mass evacuations and time-sensitive raids.

The current weight of the biometric equipment is an issue when it must be carried on foot into the field. [12] When faced with carrying a lot of weight already, it may be tempting to leave the equipment behind.

Recommendations on technical issues:

1. Develop a roadmap for providing seamless interoperability between DoD biometric systems, and then between DoD and non-DoD biometric systems.

2. Develop a roadmap for reducing the amount of time it takes to get a response from a query to a remote server.
3. Develop methods of quick enrollment for those situations that require it.
4. Develop lighter-weight mobile biometric systems.

5 Imagining the Future

The following describe some technological advances that may be considered as the futuristic mobile biometric collection device.

1. Storage
   An effort to imagine the ideal futuristic setup for collecting biometrics in the field begins with storage devices that are so small in size, yet so large in capacity that the entire FBI fingerprint database, and any other biometric database, can fit onto the equivalent of today's small USB flash drive. In such a case, one can work with more confidence that the persons currently detained are not wanted, or to quickly know past criminal activities, if any.
2. Processing
   However, to access all that data in a reasonable amount of time would require the futuristic mobile devices to make billions of biometric comparisons per second. Therefore, the processing power of mobile devices must be exponentially greater than today's mobile devices, while still using lightweight batteries that can last many hours on a charge.
3. Networking
   As powerful as the above technological steps would be, such mobile devices would be required to return to base on a regular basis to dump any new enrollments into the growing database, and to receive any new enrollments from other sources. In short, the mobile device would need to synchronize its database with a centralized database. To overcome this limitation, the future must include a satellite network (or some other method of communication) that can handle exponentially much more traffic than it does now, especially if there are a lot of these mobile devices in the field at any given time. This futuristic capability would allow mobile devices to synchronize with the central database while in the field in real time, or to make requests of a central database in real time.
4. Quick Capture
   From the end user's point of view, the futuristic mobile device would "instantaneously" acquire the required biometric data from enrollees by simply looking at the person of interest. One can imagine small mounted cameras on helmets, or other body locations, that acquire the necessary images, or some other method of "body scan" that would quickly and reliably provide the required data.
5. Biographics
   However, a quick acquisition of biometric samples would not reduce the time it takes to input the associated biographical data, such as a name, gender, etc, which currently requires someone to select or input via a keyboard. Therefore, a speech recognition system would be required to allow an enrollee to speak the biographical data, whereupon the mobile device would translate (if a foreign language), parse, and enter into the data into the appropriate fields for enrollment.

Recommendations on future technical issues:

1. Keep abreast of, or fund the research of, advances in storage capacity, processing power, and networking capabilities.
2. Fund research into quickly capturing biometric data.
3. Fund research into speech recognition and translation that does not require a pre-enrolled voice sample.
4. Consider how such technological advances would change the way the DoD collects biometrics when interacting with people in a combat zone or humanitarian efforts.

6 Conclusions and Technical Recommendations

The measure of universality is important because the DoD does not know ahead of time where in the world troops may be deployed. Therefore, the choice of modality is critical to ensure that it may be used within any population, and in any environment. It would not be wise to depend on a single modality because of the potential for unforeseen problems. Therefore, at least two uncorrelated modalities should be used on a regular basis, which will also help improve the accuracy of comparisons. [71]

Among other things, Table 2 shows the rating for collectability for many modalities. Table 4 shows a subjective rating of how the collectability rating might look if different environments were considered individually, based on the information already presented. The table emphasizes that the current technical challenges are the cold, wet and sandy environments.

Table 4 Modality Ratings for Environment Conditions
(H=high, M=medium, L=low, where H means that the modality deals with the environment well)

Modality	Normal	Hot	Cold	Wet	Dry	Sandy Dusty
Fingerprint	M	M	L	L	M	L
Iris	H	H	H	M	H	L
Palmprint	M	M	L	L	M	L
Palm Vein	H	H	L	H	H	M
Voice	M	H	M	L	H	L
Face	H	H	L	L	H	L
DNA	H	M	H	L	H	H

General Technical Recommendations

The previous sections outlined recommendations per environment and per modality, which are not repeated here. The following recommendations are provided as overall technical guidance into future operations:

1. Continue to acquire pictures of faces, minimally for human confirmation, but potentially for future automated matching.

2. Continue to acquire irises because they are easy to acquire, very accurate, provide very fast matching capabilities, and they can work well in the cold and in most humid environments.
3. Continue to acquire fingerprints for forensic purposes, i.e., latent prints left on the fragments of a roadside bomb.
4. Overcome the challenges with the sandy and dusty environments. This may include overcoming the problems with the modalities currently used by the DoD, or by adding a modality that performs well in such an environment while retaining high accuracy. Even though the DNA modality shows that it is rated as a high in such environments, it is not a good solution because of slow enrollment times.
5. Consider the difference in logistics when biometrics are used in mass evacuation and relief operations as opposed to in-country deployments. Should the same devices be used for all scenarios? Is speed of enrollment a higher priority than accuracy in some scenarios? Is it mandatory that the modality being used for enrollment is supported by the FBI database?

References

[1] A. Jain, A, Ross. "Introduction to Biometrics," in *Handbook of Biometrics*, A. Jain, P. Flynn, A. Ross. New York: Springer, 2008, pp. 1-41.

[2] International Biometric Group. *Comparative Biometric Testing: Round 7 Public Report, v1.2.* New York: International Biometric Group, 2009, pg. 19.

[3] 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, October 2007, Tech. Rep. NISTIR 7408, pg. 5.

[4] R. Das. "Retinal Recognition: Biometric Technology in Practice" in *Keesing Journal of Documents and Identity*, issue 23, pp. 11-14, 2007.

[5] National Research Council. *The Evaluation of Forensic DNA Evidence.* Washington, D.C: National Academy Press, 1996, pg. 16.

[6] National Institute of Justice. *The Future of Forensic DNA Testing.* Washington, D.C: U.S. Department of Justice Office of Justice Programs, 2000.

[7] J. Butler. *Forensic DNA Typing,* 2nd ed. Burlington, MA: Elsevier Academic Press, 2005, pp. 413-430.

[8] A. Jain, R. Bolle, S. Pankanti. *Biometrics: Personal Identification in Networked Society*. New York: Springer, 1996, pg 16.

[9] Department of Defense. *Test Method Standard: Environment Engineering Considerations and Laboratory Tests*. MIL-STD-810G. October, 2008.

[10] Report of the Defense Science Board Task Force on Defense Biometrics. Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics. March 2007. [On-line]. Available: http://www.acq.osd.mil/dsb/reports/ADA465930.pdf [July 19, 2010].

[11] Environment Canada. *Wind Chill Fact Sheet.* [On-line]. Available: http://www.msc-smc.ec.gc.ca/education/windchill/windchill_fact_sheet_aug_10_e.cfm. [April 6, 2010].

[12] "Interview with a Marine Officer deployed to Iraq in 2008 and Afghanistan from 2009 to 2010," interview conducted on August 6, 2010.

[13] Energizer. *Alkaline Manganese Dioxide Handbook and Application Manual*. Version 1.3, 2008. [On-line] Available: data.energizer.com/PDFs/alkaline_appman.pdf [April 5, 2010].

[14] Stewart, R. F., Estevao, M., and Adler, A. 2009. "Fingerprint recognition performance in rugged outdoors and cold weather conditions." *Proceedings of the 3rd IEEE international Conference on Biometrics: theory, Applications and Systems* (Washington, DC, USA, September 28 - 30, 2009). IEEE Press, Piscataway, NJ, 300-305.

[15] Victoria Forensic Science Centre. *Duration of Latent Impressions*. June, 2002. [On-line] Available: http://www.nifs.com.au/F_S_A/Duration of latent fingerprints.pdf. [April 6, 2010].

[16] D. Johnson. (2004, December 28). "Digital Focus: Cold Weather Photo Survival Guide." *PC World*. [On-line]. Available: http://www.pcworld.com/article/118862/digital_focus_cold_weather_photo_survival_guide.html. [April 6, 2010].

[17] S. Im, H. Choi, *A Filter Bank Algorithm for Hand Vascular Pattern Biometrics*, Proceedings of Seventh International Conference on Control, Automation, Robotics and Vision (ICARDV 2002), Dec. 2002, Singapore, pp. 776-781.

[18] A. Choi, C. Tran. "Hand Vascular Pattern Technology," in *Handbook of Biometrics*, A. Jain, P. Flynn, A. Ross. New York: Springer, 2008, pp. 253-270.

[19] J. Butler. *Forensic DNA Typing,* 2nd ed. Burlington, MA: Elsevier Academic Press, 2005.

[20] S. Chowhan, G. Shinde, *Iris Biometrics Recognition Application in Security Management*, 2008 Congress on Image and Signal Processing, pp. 661-665.

[21] After Action Report, II MEF Biometrics Townhall Conference, April 2, 2008. [On-line] Available: https://www.mccll.usmc.mil. [July 1, 2010].

[22] "Interview with a Marine Officer in Afghanistan from 2009 to 2010," interview conducted on August 9, 2010.

[23] B. Moran. "DNA Sampling Made Easy," in *Forensic Magazine.* April/May 2010.

[24] C. Champod, C. Lennard, P. Margot, M. Stoilovic. *Fingerprints and Other Ridge Skin Impressions.* Boca Raton, FL: CRC Press, 2004.

[25] H. Fakourfar, S. Belongie. *Fingerprpint Recognition System Performance in the Maritime Environment.* [On-line]. Available: http:// vision.ucsd.edu/sites/default/files/PID1036733.pdf. [May 4, 2010].

[26] S. Modi, S. Elliott. "Impact of Image Quality on Performance: Comparison of Young and Elderly Fingerprints," in *Proceedings of the 6th International Conference on Recent Advances in Soft Computing (RASK 2006)*, 2006, pp. 449-454.

[27] T. Mansfield, G. Kelly, D. Chandler, J. Kane. (2001, March 19). *Biometric Product Testing Final Report.* Centre for Mathematics and Scientific Computing, National Physical Laboratory. [On-line]. (Issue 1.0). Available: http://www.cesg.gov.uk/policy_technologies/biometrics/media/biometrictestreportpt1.pdf. [April 9, 2010].

[28] *Evaluation Report, Biometrics Trial, 2b or not 2b.* Ministry of the Interior and Kingdom Relations. 2005.

[29] S. Modi, S. Elliott, J. Whetstone, H. Kim. "Impact of Age Groups on Fingerprint Recognition Performance," in *IEEE Workshop on Automatic Identification Advanced Technologies (AutoID)*, 2007, pp. 19-23.

[30] A. Jain, L. Hong, S. Pankanti, R. Bolle. "An Identity-Authentication System Using Fingerprints", in *Proceedings of the IEEE*, vol. 85, No. 9, pp. 1365-1388.

[31] M. Frick, S. Modi, S. Elliott, E. Kukula. "Impact of Gender on Fingerprint Recognition Systems," in *The 6th International Conference on Information Technology and Applications (ICITA)* 2008, pp. 717-721.

[32] "Crimes and Myth-demeanors," in *Mythbusters.* Collection 2, Disc 1. 2007.

[33] Reliance on Iris Scanner for Biomtrics-Based Indigenous Administrative Management, April 28, 2005. [On-line] Available: https://www.mccll.usmc.mil. [August 9, 2010].

[34] R. Kremen. "Touchless 3-D Fingerprinting," *Technology Review*, Sep. 30, 2009. [On-line]. http://www.technologyreview.com/computing/23549/page1/ [July 16, 2010].

[35] Y. Chen, G. Parziale, E. Diaz-Santana, and A. Jain, " 3D Touchless Fingerprints: Compatibility with Legacy Rolled Images", *Proc. of Biometric Symposium, Biometric Consortium Conference*, Baltimore, September, 2006.

[36] Fast Tenprint Capture, http://www.nist.gov/itl/iad/ig/ft_capture.cfm [July 8, 2010].

[37] R. Roizenblatt, P. Schor, F. Dante, J. Roizenblatt, R. Belfort Jr. *Iris Recognition as a Biometric Method after Cataract Surgery.* [On-line]. Available: http://www.biomedical-engineering-online.com/content/3/1/2. [April 27, 2010].

[38] J. Wayman, N. Orlans, Q. Hu, F. Goodman, A. Ulich, V Valencia. (2008, October). *Technology Assessment for the State of the Art Biometrics Excellence Roadmap.* MITRE Technical Report. Vol. 2, Ver. 1.2.

[39] P. Tome-Gonzalez, F. Alonso-Fernandex, J. Ortega-Garcia. "On the Effects of Time Variability in Iris Recognition," in *2nd International Conference on Biometrics: Theory, Applications and Systems*, 2008, pp. 1-6.

[40] S. Baker, K. Bowyer, P. Flynn. "Empirical Evidence for Correct Iris Match Score Degradation with Increased Time Lapse Between Gallery and Probe Images," in *International Conference on Biometrics*, June, 2009, pp. 1170-1179.

[41] P. Corby, et.al. "Using Biometrics for Participant Identification in a Research Study: a Case Report." The Journal of the American Medical Informatics Association, Vol. 13, No. 2, pp. 233-235.

[42] J. Daugman. *How Iris Recognition Works.* [On-line]. Available: www.cl.cam.ac.uk/ ~jgd1000/ irisrecog.pdf. [April 28, 2010].

[43] P. Phillips, P. Flynn. "ICE Mining: Quality and Demographic Investigations of ICE 2006 Performance Results," presented at *Multiple Biometrics Grand Challenge Kick-Off Workshop.* April, 2008. [On-line]. Available: http://face.nist.gov/mbgc/ ICE_Mining_PJF_080417.pdf. [April 28, 2010].

[44] K. Hollingsworth, K. Bowyer, P. Flynn. "Pupil Dilation Degrades Iris Biometric Performance," in *Computer Vision and Image Understanding*, Volume 113, Issue 1, January 2009, pp. 150-157.

[45] D. Sidlauskas, s. Tamer. "Hand Geometry Recognition," in *Handbook of Biometrics*, A. Jain, P. Flynn, A. Ross. New York: Springer, 2008, pp. 91-107.

[46] D. Davis, et.al. (2008, October). *Technology Assessment for the State of the Art Biometrics Excellence Roadmap.* MITRE Technical Report. Vol. 1, Ver. 1.2.

[47] I. Sarkar, F. Alisherov, T. Kim, D. Bhattacharyya. "Palm Vein Authentication System: A Review." International Journal of Control and Automation, Vol. 3, No. 1, March, 2010, pp. 27-34.

[48] *Vocal Cord Disorders*. The University of Chicago Medical Center. [On-line]. Available: http://www.uchospitals.edu/online-library/content=P00475. [May 7, 2010].

[49] D. Lindsay, P. Jack, M. Christian. "Other-Race Face Perception," in *Journal of Applied Psychology*, vol. 76., No. 4, pp 587-589, 1991.

[50] K. Tanaka, K. Machida, S. Matsuura, S. Akamatsu. "Comparison of Racial Effect in Face Identification Systems based on Eigenface and GaborJet," in *SICE Annual Conference*, 2004, pp 669-674.

[51] P.J. Phillips, H. Moon, S. Rizvi, P. Rauss. "The FERET Evaluation Methodology for Face-Recognition Algorithms," in *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 22, No. 10, Oct. 2000, pp. 1090-1104.

[52] FG-NET Aging Database. [On-line]. Available: http://www.fgnet.rsunit.com. [April 23, 2010].

[53] K. Ricanek, T. Tesafaye. "MORPH: A Longitudinal Image Database of Normal Adult Age-Progression," in *IEEE 7th International Conference on Automatic Face and Gesture Recognition*, Apr. 2006, pp. 341-345.

[54] D. Blackburn, M. Bone, P. Phillips. (2001, February 2001). *Facial Recognition Vendor Test 2000, Evaluation Report.* [On-line]. Available: http://www.frvt.org/DLs/FRVT_2000.pdf. [April 13, 2010].

[55] P. Phillips, P. Grother, R. Michaels, D. Blackburn, E. Tabassi, J. Bone. *Face Recognition Vendor Test 2002: Overview and Summary*. [On-line]. Available: http://www.frvt.org/DLs/FRVT_2002_Overview_and_Summary.pdf. [April 14, 2010].

[56] Y. Fu, G. Guo, T. Huang. "Age Synthesis and Estimation via Faces: A Survey," in *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 2008.

[57] E. Kukula, S. Elliott. (2004). *Evaluation of a Facial Recognition Algorithm Across Three Illumination Conditions.* IEEE Aerospace and Electronic Systems Magazine. Vol 19, Number 9, September 2004.

[58] U.S. Department of State. *How to Apply [for a Passport] in Person.* [On-line]. Available: http://www.travel.state.gov/passport/get/first/first_830.html. [April 13, 2010].

[59] The AR Face Datbase. [On-line]. Available: http://cobweb.ecn.purdue.edu/~aleix/aleix_face_DB.html. [April 23, 2010].

[60] *Face Recognition Format for Data Interchange.* (2004). American National Standards Institute, Inc., Information Technology Industry Council. ANSI/INCITS 385-2004.

[61] S. Li, R. Chu, S. Liao, L. Zhang. (2007) *Illumination Invariant Face Recognition Using Near-Infrared Images.* IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 29, No. 4, April 2007.

[62] C. Wang, Y. Li, C. Wang. "An Efficient Illumination Compensation based on Plane-fit for Face Recognition," in *10th International Conference on Control, Automation, Robotics and Vision*, 2008, pp. 939-943.

[63] H. Sellahewa, S. Jassim. (2010). *Image-Quality-Based Adaptive Face Recognition.* IEEE Transactions on Instrumentation and Measurement, Vol. 59, No. 4, April 2010.

[64] N. Awekotuku, "Mata Ora: Chiseling the Living Face: Dimensions of Maori Tattoo," in *Sensible Objects: Colonialism, Museums and Material Culture*, E. Edwards, C. Gosden, R. Phillips. New York: Berg, 2006, pp. 121-140.

[65] Biometrics – Jurisdictional and Societal Considerations for Non-Government Applications – Part 2: Specific Technologies and Practical Applications (Draft). ISO/IEC. 24714-2. 2008.

[66] J. Butler. *DNA Quality in the Context of Biometrics.* Biometric Quality Workshop II. [On-line]. Available: http://biometrics.nist.gov/quality/workshop07/proc/butler_Biometrics_DNA_Quality_Nov2007.pdf. [April 22, 2010].

[67] J. Woodward. "Using Biometrics to Achieve Identity Dominance in the Global War on Terrorism." *Military Review,* September-October 2005, pp. 30-34.

[68] D. Shontz. *DNA as Part of Identity Management for the Department of Defense.* RAND National Defense Research Institute. 2010. [On-line]. Available: http://www.**rand**.org/pubs/occasional_papers/**2010**/**RAND**_OP286.sum.pdf. [August 3, 2010].

[69] "Interview with a biometrics expert in USSOCOM," interview conducted on July 27, 2010

[70] "Interview with an Army Officer deployed to Afghanistan in 2009," interview conducted on August 5, 2010.

[71] A. Ross, K. Nandakumar, A. Jain. "Introduction to Multibiometrics," in *Handbook of Biometrics*, A. Jain, P. Flynn, A. Ross. New York: Springer, 2008, pp. 271-292.

Appendix A Climatic Design Types

Figure 1 shows the world and how climatic design types, introduced in Table 3, have been assigned by the DoD.

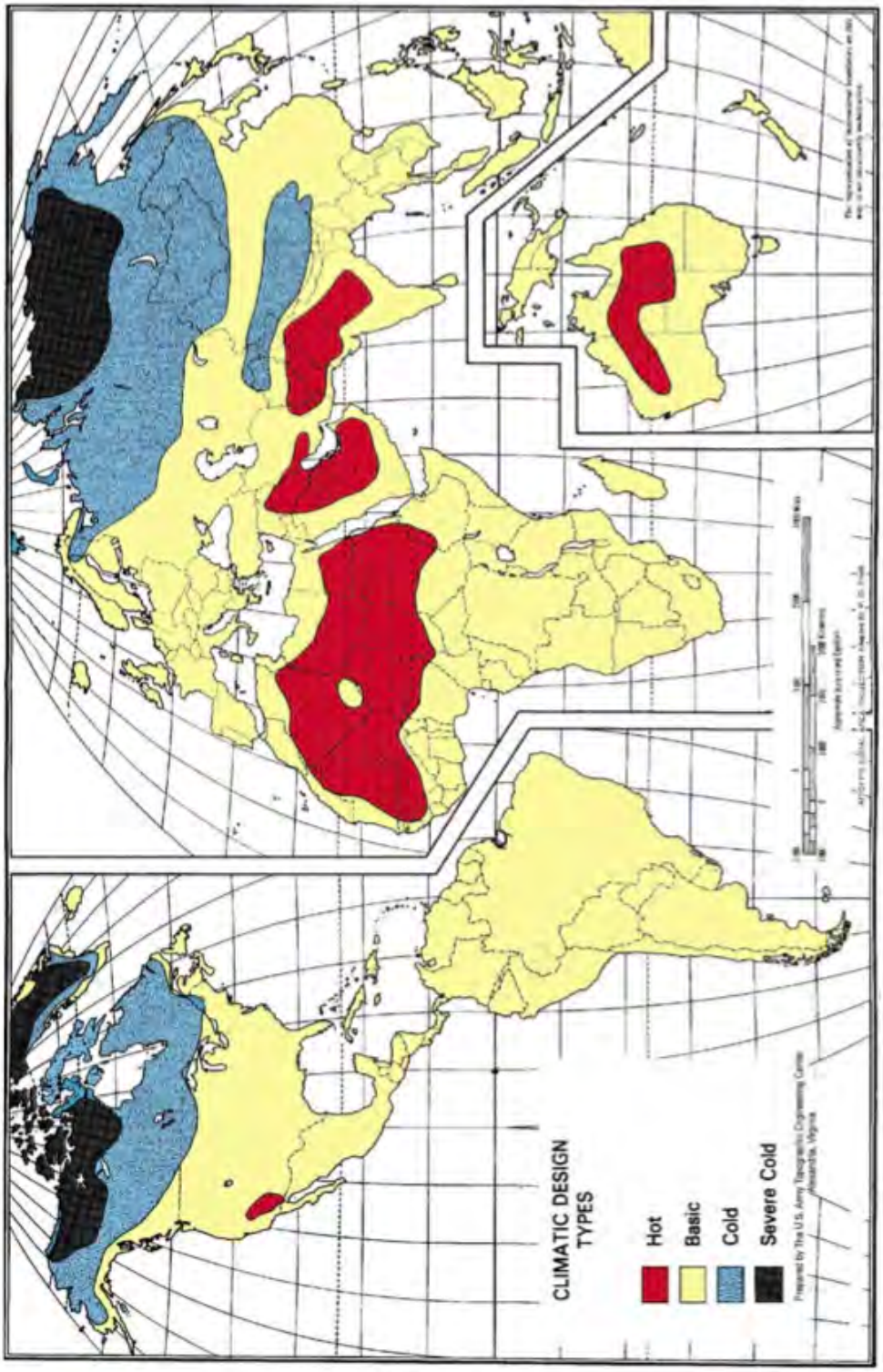

Figure 1 Areas of Occurrence of Climatic Design Type (From [9])

Appendix B Minimum Temperatures

Figure 2 shows the world and how the DoD has assigned the cold climatic design types, introduced in Table 3.

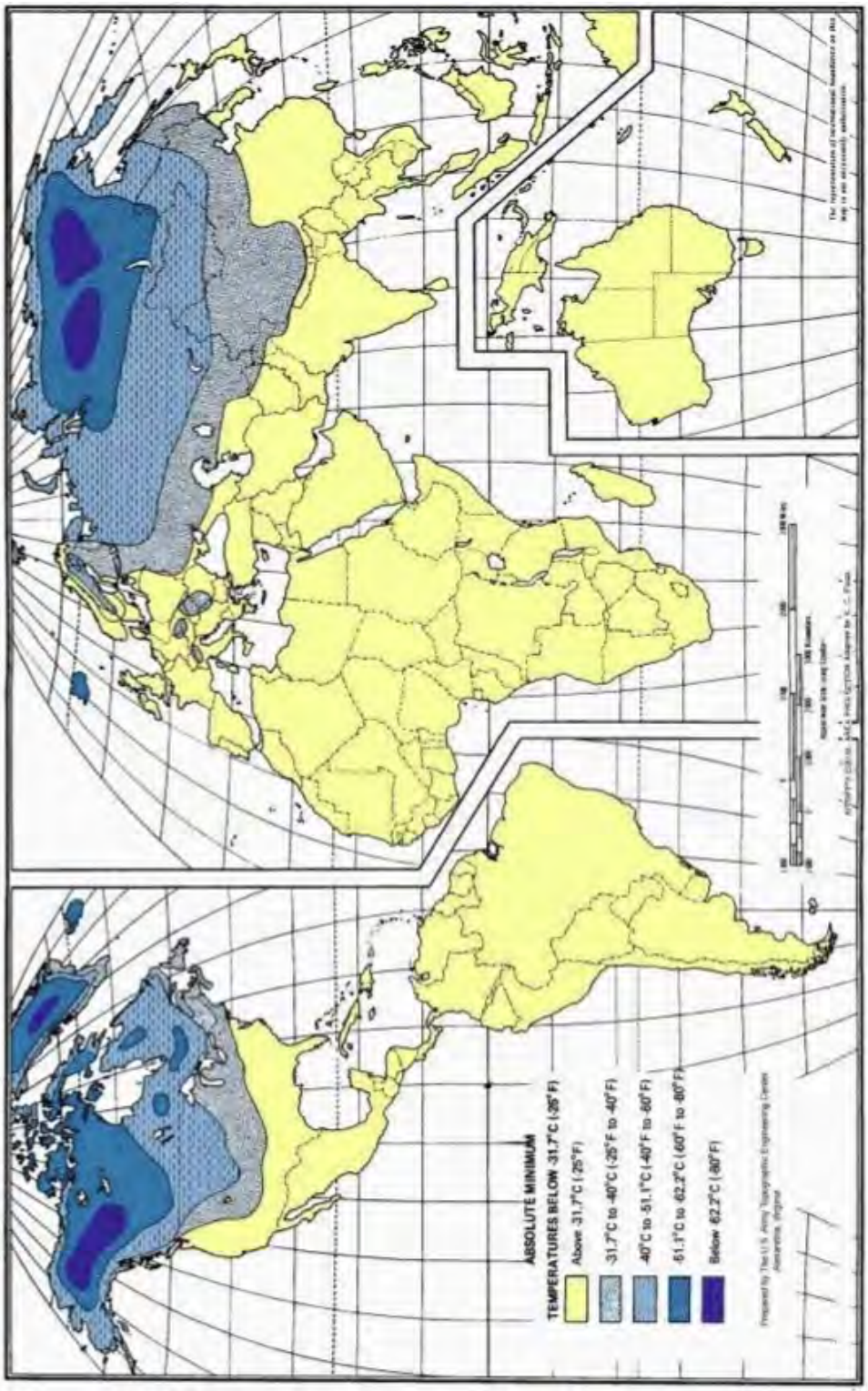

Figure 2 Distribution of Absolute Minimum Temperatures (From [9])

Appendix C Maximum Temperatures

Figure **3** shows the world and how the DoD has assigned the hot climatic design types, introduced in Table 3.

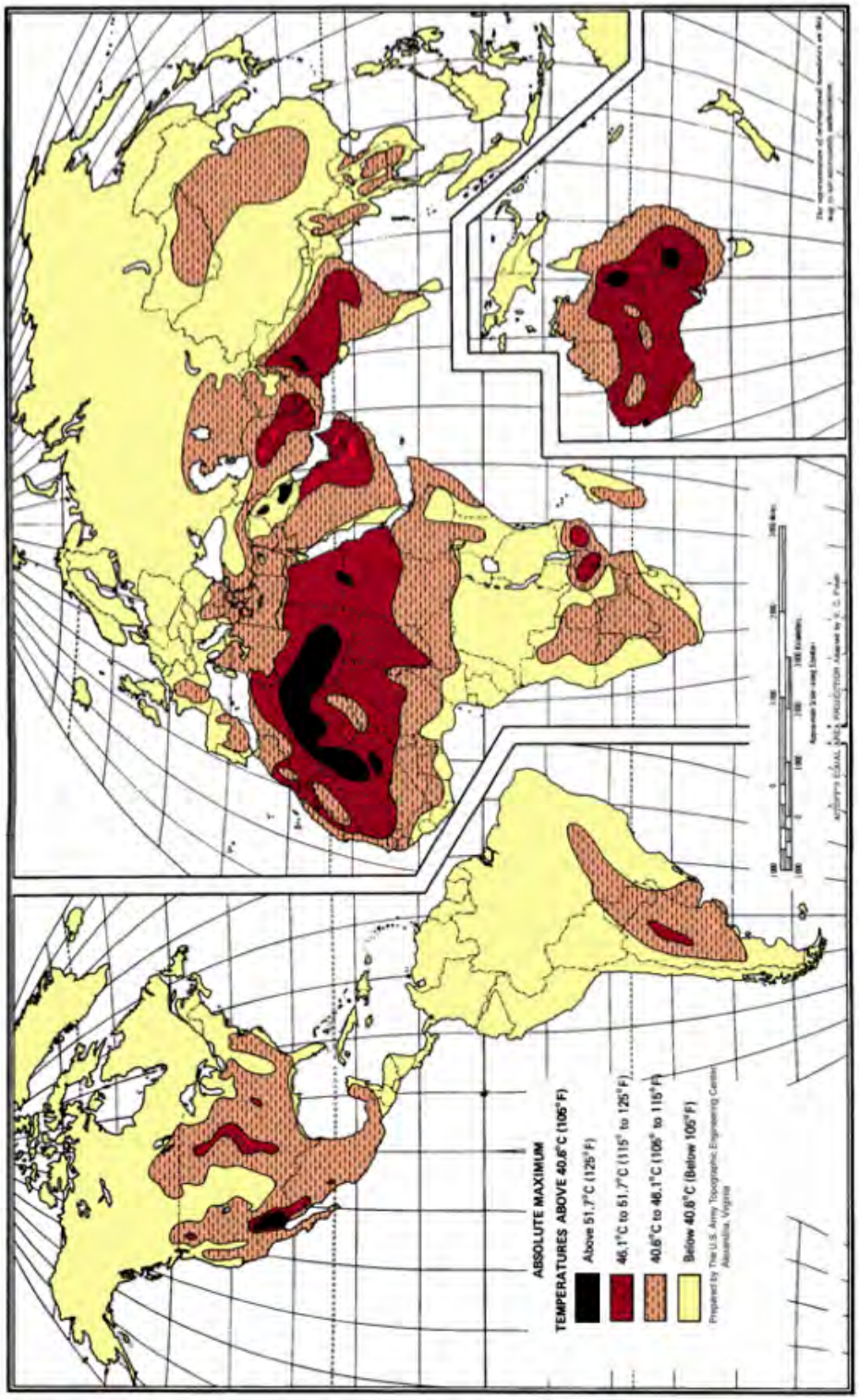

Figure 3 **Distribution of Absolute Maximum Temperatures (From [9])**

Part II
Culture and Biometric Data Gathering: Constraints and Opportunities

Heather S. Gregg, PhD

This page is intentionally blank.

Part II
Culture and Biometric Data Gathering: Constraints and Opportunities

Heather S. Gregg, PhD

A critical component to the U.S. military's successful collection of biometric data on populations is their willingness to comply with data gathering. This section considers, broadly, how culture might affect the success and ease of collecting biometrics in current and future deployments.

The section begins by defining culture and how it shapes perceptions and behavior. It asserts that culture alone will not predict a population's response to biometrics technology, but that the context in which biometric data is gathered matters significantly for how a population will react. Understanding the dynamic between culture and specific contexts, therefore, will yield better predictive results for a population's compliance to biometric technology. The section builds on this discussion to offer a brief outline of existing literature on populations' perceptions of biometric technology and concerns surrounding its use, focusing specifically on western concerns over privacy and data management. The section then uses interviews to describe four scenarios for gathering biometrics and how culture and context affect these scenarios—data collection on entire villages and urban centers; collecting data on those seeking jobs, healthcare, food and other incentives; registering foreign nationals being trained as part of Security Forces Assistance (SFA); and enrolling visitors to the United States. The section concludes by offering questions that U.S. military operators can investigate about a population prior to gathering data to assess their willingness to comply with biometrics technology.

The Dynamic between Culture and Context

Culture is not an easy term to define. Most definitions suggest that it is extremely broad and consists of various subparts. Perhaps one of the oldest definitions of culture comes from E. B. Taylor who described it as "that complex whole which includes knowledge, belief, art, morals, law, custom, and any other capabilities and habits acquired by man as a member of society."[1] Of particular utility to the U.S. military is the Marine Corps' *Operational Culture for the Warfighter*, which defines culture in five subparts: it is shared; it shapes a group's worldview; aspects of culture are interconnected; it varies over time and across areas; and it is dynamic.[2]

The *Operational Culture for the Warfighter* definition stresses, first of all, that culture exists at the group level. An individual's culture is shaped by the groups in which he or she interacts. It is important, therefore, to investigate culture at the group level.

[1] E.B. Taylor, *Primitive Culture*, London: John Murray, 1871, p. 1
[2] Barak A. Salmoni and Paula Holmes-Eber, *Operational Culture for the Warfighter*, Quantico: Marine Corps University Press, 2009, p. 36

However, in most cases, individuals belong to more than one group and each group has its own culture which shapes individual behavior. Furthermore, subcultures can exist within wider cultures that have their own distinct norms and forms of behavior.[3] Thus, understanding how culture shapes individual preferences and behaviors is more complicated than just looking at the national level; subcultures and other levels also need to be considered.[4]

When investigating culture and how it might affect military operations, it is also important to keep in mind that how outsiders see and understand a group's culture may be different from how the insider views his or her own culture. Many aspects of culture exist at the subconscious level and those within the group may not be able to identify or explain patterns of behavior consciously. Likewise, those outside the culture have their own cultural perspectives and biases, which shape the way they see other groups' cultures. How one group sees and defines another, and how a group sees itself may, therefore, be quite different.[5]

Operational Culture further asserts that some aspects of culture can be mapped or measured, while others cannot. For example, it is possible to map religious affiliation, gender, age groups, and possibly race (although race is often subjective). However, many aspects of culture are not mapable, such as worldviews and culturally generated perceptions, both of which are important considerations for biometric data gathering. Human terrain mapping, therefore, has its limits because it cannot capture some of most important the aspects of culture for biometric data gathering.

Perhaps the most important aspect of culture outlined in *Operational Culture* is that culture is not a constant; culture changes over time and reacts to changes in the political, social and physical environment. Culture, in other words, is dynamic. For example, economist Jeffry Sachs observes that, when trying to explain why some regions develop economically faster than others, looking only at that region's culture will not yield fruitful results. Rather, Sachs recommends looking at three clusters of variables: the environment, which includes things like access to waterways, fossil fuels, climate, and disease; the socio-political environment, including governmental ideologies and policies, war, famine, and the legacy of previous political systems; and the culture of ideas and innovation, which stem from education, freedom of ideas, information technology and

[3] For more on subcultures, see: Marvin Wolfgang and Franco Ferracuti, *The Subculture of Violence: Towards an Integrated Theory in Ccriminology*, London: Tavistock Publications, 1967. For an overview of the theory, see: "Marvin Wolfgang's Subculture of Violence Theory," http://www.criminology.fsu.edu/crimtheory/wolfgang.htm, as of July 12, 2010.

[4] Several scholars have developed national and civilizational level characterizations of culture, including Geertz Hofstede's five constructs that characterize national culture, and Samuel Huntington's hypothesis that civilizations, which sit above national culture, are responsible for group behavior. See: Geertz Hofstede, *Culture's Consequences: Comparing Values, Behaviors, Institutions, and Organizations Across Nations*, second edition, New York, Sage Publications, 2001; and Samuel Huntington, *The Clash of Civilizations and the Remaking of World Order*, New York: Simon and Schuster, 1996.

[5] Salmoni and Holmes-Eber, p. 35.

even property rights.[6] Culture, for certain, is present in all of these variables. However, it does not operate independently of its surroundings but, rather, shapes and is shaped by society, politics and the environment.

The observation that culture reacts to context is particularly important for biometric data gathering because it suggests that assessing culture by itself, without considering the specific circumstances in which biometric data gathering occurs, will not yield an accurate prediction of how the population will respond. This is particularly true of U.S. military operations. In most cases, the military will be operating in countries that have either an armed conflict or the potential for armed conflict. These countries will most likely already be in a period of social, political and cultural flux. Groups of people could be uprooted from their homes and made internally displaced or refugees, changing not only their social, political, and physically surroundings but also their culture. Chronic violence can also alter a group's culture and create a subculture that, although connected to the wider culture, has its own set of norms, values, and behaviors.[7]

Moreover, the very presence of U.S. military personnel in the country could cause the culture to change. "Going in big" with large numbers of troops and equipment, like the United States did in Iraq and Afghanistan, undoubtedly has changed these countries' cultures. Military operations in both countries have resulted in new governments, new forms of law and security forces, changes in the economy, and the renewal or spread of education. These changes to governance and society have undoubtedly altered the culture.

Thus, for the purpose of biometric data gathering, it is essential to consider the social, political, and security environment; the conditions under which the data is being gathered (such as a conflict zone); and how the presence of U.S. forces is changing society and culture.

Literature on Culture and Biometrics

The literature on culture and biometrics is thin relative to other topics, like the science behind the technology or data management.[8] Most of the articles that do exist on culture and biometrics focus on the role that popular perceptions play in accepting and trusting biometric technology. As will be discussed, these articles reveal that a population's openness to biometrics has more to do with education on the technology and expectations on rights to privacy, than it does culture.

Perhaps the most widely researched region for popular perceptions of biometric technology is Europe. Governments, non-governmental organizations, and commercial

[6]Jeffry Sachs, "Notes on a New Sociology of Economic Development," *Culture Matters: How Values Shape Human Progress*, Lawrence E. Harrison and Samuel P. Huntington, eds., New York: Basic Books, 2000, pp. 29-43.
[7] Wolfgang and Ferracuti.
[8] For example, there are journals devoted to biometrics, *Biometrics*, founded in 1945, and *Biometrics Technology Today*. The latter only produced 16 results for articles with the word culture in it. See: http://www.biometrics.tibs.org/, and http://www.elsevierscitech.com/nl/btt/home.asp, respectively, as of July 14, 2010.

retailers have surveyed populations in order to better understand the acceptance of biometric technology throughout the European Union. For example, a 2004 article used survey data to investigate popular perceptions of Radio Frequency Identification (RFID) implants and biometric technology more broadly. It found that, although Europeans were not familiar with RFID, they had concerns about privacy and data safety of biometrics. However, the authors also report that biometric technology is gaining acceptance in Europe, particularly as the threat of terrorism and identity theft are on the rise, and because of the convenience that the technology provides. The same article distributed a survey to students in two Massachusetts colleges regarding biometric technology and found similar results to those in Europe.[9]

A 2005 paper on the creation of e-Passports within the European Union used media content analysis within five European countries (Germany, Great Britain, Spain, Denmark and Greece) and five non-European countries (Malaysia, USA, Taiwan, South Korea and Japan) to gauge national perceptions of this use of biometric technology. The authors found that countries with an adequate amount of education on the utility and benefits of biometrics were more accepting of the technology. The report concludes: "Overall, the socio-technical opinion measurement revealed that to educate a population on the necessity for greater security is a time and technology intensive process. It could require many years to develop from initial parliamentary discussion over a functioning infrastructure to the actual product launch."[10] In other words, conditioning—not culture—is the key to determining a population's positive perception of biometric technology.

In 2009 the Irish Council for Bioethics issued a position paper which considers the ethical, social and legal issues of biometric technologies, including the collection, use and storage of biometric data. The report argues that:

> In the Council's opinion, the justification of implementing a biometric application is reliant on the application being considered proportionate. Biometric applications should, therefore, be assessed on a case-by-case basis, which involves a consideration of the relevance and necessity of employing biometric technologies, given the proposed purpose of the system, the environment in which it will be used, and the level of efficiency and degree of reliability required to achieve the proposed purpose.[11]

The report continues by arguing that, in order to gain the trust of the population, transparency between the government and the population needs to be established and

[9] Christine Peraklis and Robert Wolk, "Social Acceptance of RFID as a Biometric Security Method," *IEEE Society and Technology Magazine*, Fall 2006, pp. 35-42.
[10] Grace Ng-Kruelle, Paul A. Swatman, J. Felix Hampe, and Douglas S. Rebne, "Biometrics and E-Identity (E-Passports) in the European Union: Overcoming PoC Cultural Diversity for Common Cause?" *IADIS International Conference e-Society 2005*, available at: http://www.iadis.net/dl/final_uploads/200505C028.pdf, as of July 13, 2010.
[11] "Biometrics: Enhancing Security or Invading Privacy?" *Irish Council for Bio Ethics*, 2009, available at: http://www.bioethics.ie/uploads/docs/Final_Biometrics_Doc_HighRes.pdf, as of July 13, 2010. Quote taken from p. vii.

honest debate on the dangers associated with biometric data gathering and storage needs to occur.[12]

These articles yield another area of relevance to populations' acceptance and compliance with biometric data gathering—ethics. A 2003 article from *Ethics and Information Technology* lays out the tradeoffs between the security that biometric information can provide, and the technology's potential impact on privacy.[13] The author argues that biometric identification poses risks to an individual's privacy through harm or harassment that may come from the government or commercial businesses that have access to personal information, through unintended and unauthorized use of the data, and for the potential theft of the data and the harm that could come from the release of biometric information. The author concludes that, given the potential to harm an individual's privacy, the use of biometric technology should not be mandatory for social privileges, such as a driver's license, and commercial use of biometric data gathering should clearly explain the risks associated with voluntarily giving that information.[14]

In Europe, several agencies have been stood up to discuss and safeguard privacy and other ethical concerns regarding biometric data gathering. The European Biometrics Forum was created as a non-governmental interest group to coordinate awareness and concerns around biometric data gathering. Also within Europe, HIDE, the Homeland Security, Biometric Identification & Personal Detection Ethics, was created in 2008 "to set up a platform devoted to ethical and privacy issues of biometrics and personal detection technologies which addresses transnational (European) and international problems."[15] RISE, the Rising Pan European and International Awareness of Biometrics and Security Ethics, is another European led initiative that aims to increase international awareness and dialogue on biometrics and ethics.[16]

The United States has a similar relationship to biometric technology as does Europe. Alterman notes that, prior to September 11th, the U.S. population was leery about biometric technologies. For example, in 2001, Tampa city police used facial recognition technology on attendees of the Super Bowl to search for criminals and possible terrorists. This use of biometric technology stirred debates over the legal limits of conducting surveillance on the general population without evidence of wrongdoing, along with privacy issues and civil liberties in biometric screening.[17] Similar to Europe, advocacy and watchdog groups, such as the American Civil Liberties Union, have taken up the cause of biometrics and ethical concerns surrounding its use in the United States.[18]

---

[12] "Biometrics: Enhancing Security or Invading Privacy?"
[13] Anton Alterman, "'A Piece of Yourself": Ethical Issues in Biometric Identification," *Ethics and Information Technology*, Vol. 5, 2003, 139-150.
[14] Alterman, pp. 147-149.
[15] For more on HIDE, see: http://www.hideproject.org/, as of July 13, 2010.
[16] For more on RISE, see: http://www.riseproject.eu/, as of July 13, 2010.
[17] Alterman, p. 142. See also: John Woodward, Jr. "Super Bowl Surveillance: Facing Up to Biometrics," *RAND Issue Papers*, May, 2010, available at http://www.rand.org/pubs/issue_papers/IP209/index.html, as of August 31, 2010.
[18] See, for example: "ACLU Testifies to Congress on Dangers of Biometric Passports," available at http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-60594, as of July 14, 2010.

However, following September 11th, "the attack and subsequent threats posed by Al Qaeda changed public attitudes rapidly: airports announced near-term implementation of scanning programs, federal agencies undertook expedited reviews of biometrics-based security systems, and stocks of biometrics vendors shot up."[19] Another threat, consumer security, has also changed public attitudes towards biometric identification. Unisys, a private-for-profit company, finds that acceptance of biometric technology to protect against bank fraud and prevent identity theft is on the rise, not only in the United States but in the other countries they surveyed.[20] However, ethical questions about biometric technology persist in the United States.

Articles on countries outside of Europe reveal more openness to the technology and its many uses. A 2009 article from *AI and Society*, for example, outlines findings from a survey that aims to measure popular perceptions of biometric data gathering in three countries: the United Kingdom, India, and South Africa.[21] The article asked respondents about their perceptions of biometric data gathering in relation to health concerns, loss of privacy, and basic knowledge of the technology itself. The survey found that Indians viewed the technology most favorably, while citizens of the UK had the most concerns about biometric data gathering, particularly privacy issues.[22]

A 2010 article in *Global Health Action* also offers some initial insights into populations and their willingness to submit to biometric data gathering. The article investigates fingerprint biometrics in three healthcare centers spread across two countries, South Africa and Kenya, with the aim of understanding the potential of marrying biometric identity data with healthcare data on individuals. The article reports that, overall, individuals had a high rate of compliance to biometric data gathering when connected to access to health care, above 94 percent in adults and around 50 percent for children under one year old. The report did mention that there were some who refused to give their biometric data; however, it did not report these numbers independently, nor did the authors investigate why individuals were reluctant to give that information.[23]

The brief review of literature on popular perceptions of biometric technology reveals that populations are willing to participate in biometric data gathering if the context is right. African health clinics in two countries had high compliance rates, and Europeans saw the utility of biometric technology as a counterweight to terrorist threats and identity theft. However, European perceptions of biometrics also reveal that expectations about privacy shape the way populations understand the utility and ethical

[19] Alterman, p. 148.
[20] Unisys surveys nine countries: The United States, the UK, Brazil, Australia, New Zealand, Spain, Belgium, the Netherlands, and Germany. See: "Unisys Research Shows Growing Acceptance of Biometrics Among Consumers for Protecting Identities and Personal Information," November 2009, available at: http://www.unisys.com/unisys/news/detail.jsp?id=1120000970000610143, as of July 14, 2010.
[21] Chris Riley, Kathy Buckner, Graham Johnson, David Benyon, "Culture and Biometrics: Regional Differences in the perception of Biometric Authentication Technologies," *AI & Soc*, Vol. 24, 2009, 295-306.
[22] Riley, et al, pp. 295-297.
[23] Adwoa Serwaa-Bonsu, et al, "First Experiences in the Implementation of Biometric Technology to Link Data From Health and Demographics Surveillance Systems with Health Facility Data," *Global Health Action*, Vol. 3, 2010, pp. 1-8.

application of these technology. In other words, contexts—threats and incentives—appear to shape populations' willingness to submit to biometric data gathering.

Culture and Context in Biometric Data Gathering

The previous discussion on culture and biometrics argues that culture, by itself, does not adequately predict populations' acceptance or rejection of the technology. Rather, the context in which biometrics is collected and for what ends plays a pivotal role in perceptions and compliance to biometric data gathering.

Building off of interviews from officers and civilians in the Department of Defense (DOD), and those working in the Department of Homeland Security's (DHS) US-Visit program, this section explores four distinct contexts that have shaped populations' compliance with biometric data gathering for the DOD and DHS: gathering biometrics on entire villages and urban centers; collecting data on those seeking jobs, healthcare, and food; registering foreign nationals being trained as part of Security Forces Assistance (SFA); and enrolling visitors to the United States.[24]

Overall, this research reveals that the DOD and DHS have received surprisingly little cultural resistance from populations asked to give their biometric data. However, U.S. deployments in Iraq and Afghanistan, Southeast Asia and Latin America, along with the experiences of US-Visit, do provide valuable insights for gaining populations' compliance and willingness to participate in biometric data gathering.

Context One: Gathering biometrics on entire populations

In several cases, U.S. forces have attempted to gather biometric data on entire cities or villages. One example comes from U.S. operations in Fallujah, Iraq. Fallujah, a Sunni city in Anbar province, became a center of insurgent activity, culminating with the murder and mutilation of four Blackwater contractors on March 31, 2004. U.S. Marines surrounded the city beginning on April 9 and commenced Operation Vigilant Resolve. On April 28, U.S. forces withdrew from the city following the arrangement that Iraqis would deny insurgents sanctuary in the city. Continued insurgent activity, including the growing influence of Al Qaeda in Iraq, prompted U.S. forces to reengage the city from November 7 to December 23, in Operation Phantom Furry.

Large numbers of the city's population fled as a result of both operations. In mid December, the city's inhabitants were allowed to reenter the city. At that time, Marines attempted to collect biometric data via the Handheld Interagency Identity Detection Equipment (HIIDE) and the Biometric Automatic Tool Set (BATs), in a process known as "batting." The goal was to bat all citizens and to issue identity (ID) cards that would be used to control freedom of movement. However, enrolling thousands of individuals was

[24] This section does not consider taking biometrics from detainees, because detainees do not willingly give their information.

time consuming and the process was too slow to systematically record all the returnees.[25] In 2007, Marines were still attempting to systematically bat the city and enforce the use of ID cards at check points.[26]

Other attempts were made to do biometrics on urban centers in Iraq. A Marine officer in Anbar from 2007 to 2008 and in 2009 described efforts to bat cities in his area of operation. His unit operated out of the city's Joint Security Station and were tasked with training and advising the Iraqi police, force protection, building relationships with the local population, and entering Iraqis into the Automated Biometric Identification System (ABIS). At first, hundreds of Iraqis lined up outside the police station every morning, overwhelming their capacity. To manage the numbers wishing to be batted (and receive ID cards), his team moved to "batting days," and worked more closely with local leaders to control the numbers of people wishing to be enrolled.

An Army officer deployed in Tel Afar from 2006 to 2007 also attempted to bat the city as a means of populating the ABIS database. His unit was given two HIIDE/Bats kits per company and told only to use the equipment. The officer used biometric data gathering as a means of population engagement, conversing with neighborhoods as they enrolled individuals. He noted that the population was compliant with giving their biometric information and generally understood that these efforts were designed to help catch insurgents and criminals. However, the lack of equipment and men available made the process slow and haphazard. He also stated that the information was going up into the ABIS database, but they did not have a way to check individuals against the system. Overall, his company had not received an explanation of what the equipment was good for, and so interest died. After batting the local population for several months, his company stopped because they could not see its utility.[27]

A Marine officer deployed to Afghanistan from 2009 to 2010 described an attempt to gather biometrics on a village as it returned after the Taliban was pushed out. His unit only had four Marines available to gather biometrics on the population. He noted that the population came back too quickly, and by too many different pathways to allow for systematic enrollment. He also noted that they were instructed to ask permission to take biometric information from individuals that were not detained, which was different from his time in Iraq. Overall, he believed that the effort was largely unsuccessful.[28]

Another Marine officer deployed to Afghanistan from 2009 to 2010 described efforts to create a systematic means of gathering biometrics on the population. Based on his experiences using biometric collection in Anbar province, he believed that biometrics could be useful for the fight in Afghanistan, and was essential to countering Improvised

[25] John Lettice, "Marine Corps Deploys Biometric ID Scheme," *The Register*, December 9, 2004, http://www.theregister.co.uk/2004/12/09/fallujah_biometric_id/, as of August 24, 2010.
[26] Noah Schachtman, "Iraq Diary: Fallujah's Biometric Gates (Updated)," *Danger Room: Wired,* http://www.wired.com/dangerroom/2007/08/fallujah-pics/, as of August 24, 2010.
[27] "Interview with an Army Officer deployed to Iraq from 2006 to 2007," interview conducted on August 11, 2010.
[28] "Interview with a Marine Officer deployed to Iraq in 2008 and Afghanistan from 2009 to 2010," interview conducted on August 6, 2010.

Explosive Devices (IEDs). He proposed a program where task forces would be created and would attach to operations to gather data on the population as it left the area of operation. He envisioned creating three hardened, fixed stations for men and one for women that could bat people quickly. The data collected would serve as proof of residence and provide a base to potentially identify insurgents and criminals. He requested thirty Marines to gather biometrics exclusively, freeing up war fighters for combat operations. The data collected would serve as proof of residence and provide a base to potentially identify bad guys. A company tried the idea in one operation, south of Marjah, but it was not pursued after that.[29]

Context Two: Biometrics and incentives

Incentives are a powerful means of gaining a target population's compliance. In Iraq and Afghanistan, as well as in other deployments, the U.S. military has connected biometric data gathering to a variety of incentives, including jobs, health care clinics, humanitarian assistance and identity cards. Connected incentives to biometrics is an effective means of minimizing potential cultural barriers, such as gender sensitivities, head coverings, taking photographs, and human contact.

Jobs, in particular, have provided an important context for gathering biometric data on local nationals. In most operating environments, local nationals are essential for mission success; they act as interpreters, provide human intelligence, aid security and offer support for the maintenance of life on bases. However, foreign nationals require vetting to ensure security for troops and bases; biometric technology has become one means of vetting and ensuring the identity of those given jobs.

Interviews with a biometrics expert at the Defense Biometrics Identity System (DBIDS) echo these observations. DBIDS began in Korea in the late 1990s as a means of verifying the identity of individuals entering U.S. bases, including U.S. nationals. The system expanded to Europe in 2003, then bases in USCENTCOM (except in Iraq and Afghanistan) and in Southwest Asia, and then to U.S. Air Force and other bases in the United States. The biometrics expert at DBIDS noted that foreign nationals submit to the system because they want jobs on U.S. bases. As an example, he observed that the pay is three times better in Kuwait than for manual workers connected to the oil industry. He further noted that U.S. employees have the reputation of being fair and good to their employees.[30]

An Army Special Forces officer deployed three times in Iraq between 2005 and 2008 noted that compliance in biometrics was high for those seeking employment because non-compliance would mean the loss of their job. In addition to screening all local and foreign nationals working on their base, they also did biometric collections on truck drivers crossing the Syrian border, employees at the local power plant, and those receiving contracts for goods and services. Their data collection on base workers was thorough, but, given the total number of truck drivers and electrical plant employees, not

[29] "Interview with a Marine Officer in Afghanistan from 2009 to 2010," interview conducted on August 9, 2010.
[30] "Interview with a biometrics expert at DBIDS," interview conducted on August 6, 2010.

all could be screened. Their team did random collection to act as a deterrent for potential insurgents attempting to gain access to these jobs.[31]

Perhaps the largest employment program initiated by the U.S. military was what became known as the Sons of Iraq. The Sons of Iraq took shape following the tribal "awakening" in Anbar province in late 2006. The program aimed to organize and pay Sunnis to defend their neighborhoods against Al Qaeda in Iraq. At the height of the initiative, U.S. forces had an estimated 90,000 Sons of Iraq enrolled in the program in Anbar, Diyala and Baghdad.[32]

U.S. troops gathered biometrics on the Sons of Iraq via the HIDE/Bats system. One Marine officer deployed to Anbar from July 2007 to February 2008, and again in 2009 described the process for collecting data on these ad hoc forces. The Marines worked with tribal leaders to identify and organize these forces, and others connected to tribal leaders, for "batting days," when individuals were entered into the ABIS system. He noted that no one refused to be batted, but some were nervous. Several individuals came back positive in the system, but this was not surprising because many of these men were former insurgents and detained by U.S. forces. However, the Marine officer noted that figuring out how to treat those coded as detainees became a sensitive issue for managing relationships with the local population and tribal elders, more specifically, because they were vouching for the individuals and often they were family members. Typically, these situations were handled through "commander's discretion."[33]

Aside from jobs, several officers deployed to Iraq noted that the greatest incentive for complying with biometric data gathering in Iraq was ID cards. The U.S. military issued ID cards in conjunction with biometric collection and used to monitor and control movement in several major cities in Iraq, including Baghdad, Ramadi, and Fallujah. A Marine Officer deployed to Iraq in 2007-2008 and 2009 observed that ID cards became the most valuable incentive for getting individuals batted. He noted that, more than salaries, tribal leaders would bargain for ID cards in exchange for various forms of help.[34]

A Special Forces Officer deployed to Iraq three times between 2005 and 2008 also noted the importance of ID cards to the Iraqis, stating that the Iraqis "loved" the cards.[35] Similarly, a Marine Officer deployed to Iraq in 2008 as part of a Mobile Transition Team (MiTT) said that the Iraqis really valued the identity cards that U.S. troops issued. He observed that Iraqi troops would arrive in clean uniforms to have their pictures taken and liked to have their ranks and names displayed on the cards. He

[31] "Interview with an Army Special Forces Officer deployed to Iraq from 2005-2008," interview conducted August 11, 2010.
[32] For a brief description of the Sons of Iraq initiative, see: Greg Bruno, "The Role of the 'Sons of Iraq' in Improving Security," *Washington Post*, April 28, 2008, available at, http://www.washingtonpost.com/wp-dyn/content/article/2008/04/28/AR2008042801120.html, as of August 30, 2010.
[33] "Interview with Marine Officer deployed to Anbar from 2007 to 2008, and 2009,"interview conducted on August 4, 2010.
[34] "Interview with Marine Officer deployed to Anbar from 2007 to 2008, and 2009," interview conducted on August 4, 2010.
[35] "Interview with an Army Special Forces Officer deployed to Iraq from 2005-2008," interview conducted August 11, 2010.

believed that, apart from granting freedom of movement, the badges became a status symbol in-and-of-itself.[36]

While ID cards were a valuable incentive in Iraq, they did not have the same cache in Afghanistan. A Marine officer who worked with Iraqis in 2008 and then deployed to Afghanistan from 2009 to 2010 noted that his unit tried to introduce ID cards in Helmand province but people did not know what they were (the region did not have a culture of identity cards). Furthermore, he believed that the Afghans did not understand or care about rank, the cards did not hold up in the harsh environment, and he feared that the cards would make individuals a target of the Taliban. Finally, Helmand province was rural and introducing checkpoints—and ID cards as a means of access—was not universally applicable.[37]

U.S. forces also used Medical Civil Action Programs (MEDCAPS), which provide health care to humans, in connection with biometric data gathering. An Army officer deployed to Afghanistan in 2009 stated that his unit did three MEDCAPS and gathered biometrics on all that participated. The MEDCAPS attracted women, children and the elderly in particular. He did not find any objection from participants to having their biometric data taken. He noted, though, that the MEDCAPS did not appear to get as many women as he had expected. He speculated that it was winter and most women were staying at home, as opposed to being in the fields for planting and harvesting. He also said that he had the feeling that people were avoiding events and places where biometric data gathering was taking place.[38] A Marine officer deployed to Afghanistan from 2009 to 2010 noted that his commander chose not to use MEDCAPS to enroll participants in ABIS because the Civil Affairs teams that ran these events measured their success by the number of individuals treated, and gathering biometric data slowed their progress down and possibly deterred people from coming.[39] Similarly, another Marine deployed to Afghanistan in 2009-2010 stated that his commanding officer chose not to gather biometrics in connection with MEDCAPS because he was concerned that it might compromise the mission of engaging and helping the population. He also noted that MEDCAPS cater mostly to women, the elderly and small children, who are not the ideal target (fighting age men) for the database.[40]

Finally, an Army office deployed to Tel Afar Iraq from 2006 to 2007 stated that his unit used batting as a reason for population engagement and tied it to events like humanitarian assistance. He noted that batting individuals was an opportunity to get out of vehicles and talk to people in various neighborhoods and to learn their needs and concerns. He explained to neighborhoods that batting was a means of catching terrorist

[36] "Interview with a Marine Officer deployed to Iraq in 2008 and Afghanistan from 2009 to 2010," interview conducted on August 6, 2010.
[37] "Interview with a Marine Officer deployed to Iraq in 2008 and Afghanistan from 2009 to 2010," interview conducted on August 6, 2010.
[38] "Interview with an Army Officer deployed to Afghanistan in 2009," interview conducted on August 5, 2010.
[39] "Interview with a Marine Officer deployed to Iraq in 2008 and Afghanistan from 2009 to 2010," interview conducted on August 6, 2010.
[40] "Interview with a Marine Officer in Afghanistan from 2009 to 2010," interview conducted on August 9, 2010.

and other criminals in society. He noted that they received no memorable resistance to gathering the data.[41]

Context Three: Security Force Assistance

One of the pillars of COIN doctrine is to enable the host government and local populations to fight their own insurgents. Security Force Assistance (SFA), or training and advising the host nation's security forces, has become a key component of U.S. operations in Iraq, Afghanistan, and other countries wit insurgencies, such as the Philippines and Colombia. SFA in Iraq and Afghanistan is conducted primarily through MiTT teams, which are manned by conventional forces. In addition to these operations, U.S. Special Operation Forces have engaged in Foreign Internal Defense (FID), a sub-component of SFA, as one of its primary missions since the 1970s. U.S. Special Operations Forces (SOF) conduct FID operations through U.S. State Department run Joint Combined Exchange Training (JCET) deployments and DOD run Joint Chiefs of Staff-directed exercises.[42]

Biometric data has been gathered as part of SFA through MiTT teams. As previously mentioned, U.S. forces gathered biometric data on the Sons of Iraq—ad hoc forces stood up in Anbar province, Baghadad and Diyala province—as a means of vetting and tracking these individuals. Similarly biometric data was gathered on Iraqi police and military trained by U.S. forces. A Marine officer deployed to Anbar from 2007 to 2008 remarked that his team batted around 400 Provincial Security Forces, an estimated 2,000 Sons of Iraq, and scores of Iraqi Police, for a total of around two to three thousand individuals. He noted that some of these individuals' biometric information came back as being in the system, suggesting that they had been detained by U.S. forces in the past. In situations like these, he and his team worked with the local leadership to vet these individuals.[43]

Similarly, a Marine deployed to Anbar on a MiTT team reported that they batted the entire Iraqi battalion and issued 600 ID cards. Several of the individuals came back positive in the system. He believed that some of the data collected on neighborhoods in Fallujah as part of operations in 2004 was coded en mass as "arrested". He stated that each of these individuals had to be vetted, which took time. He noted that the initial collection, and the way it was coded, significantly hindered their operations.[44]

---

[41] "Interview with an Army Officer deployed to Iraq from 2006 to 2007," interview conducted on August 11, 2010.

[42] For more on SFA, see: "Commander's Handbook for Security Force Assistance," Joint Center for International Security Force Assistance, 14 July 2008, available at http://usacac.army.mil/cac2/Repository/Materials/SFA.pdf, as of August 25, 2010; and "Joint Publication 3-07: Joint Tactics Techniques and Procedures for Foreign Internal Defense (FID)," 30 April, 2004, available at http://www.fas.org/irp/doddir/dod/jp3_07_1.pdf, as of August 25, 2010.

[43] "Interview with Marine Officer deployed to Anbar from 2007 to 2008, and 2009," interview conducted on August 4, 2010.

[44] "Interview with a Marine Officer deployed to Iraq in 2008 and Afghanistan from 2009 to 2010," interview conducted on August 6, 2010.

An Army officer deployed in Afghanistan in 2009 also gathered biometric data on the Afghan National Army in his area of operation, in addition to local defense forces (ad hoc forces similar to the Sons of Iraq), and the police. He noted that soldiers in his unit had trouble gathering biometrics on the Afghan National Army, that they saw it as a violation of trust. One Afghan commander, in particular, was unhappy that his men were being batted but U.S. forces were not.[45]

U.S. SOF has also conducted FID in Iraq and Afghanistan, as well as scores of other countries in which the United States has diplomatic ties. SOF collection of biometric data is somewhat different than with conventional forces. SOF uses the Secure Electronic Enrollment Kit (SEEK) and Cogent Systems, the systems that the majority of government agencies use, as opposed to the HIIDE/Bats system. SOF also works in countries that have varying degrees of sovereignty and rule of law; they therefore need to work through the Host Nation's government and U.S. embassies to approve operations. Given this dynamic, SOF works more closely with other U.S. government departments and agencies than do conventional forces. Finally, SOF typically trains local nationals to operate equipment and gather biometric information on their own people to minimize barriers for collection.[46]

A key means for SOF collection of biometrics data is through FID. A recent policy created at USSOCOM requires that all training that teaches U.S. Tactics Techniques and Procedures to foreign nationals be accompanied by biometric data gathering on those being trained. This policy aims to ensure that no individuals are receiving training that could be used for nefarious ends.[47]

A biometrics expert working in SOCCENT noted that connecting biometrics to FID, including JCETS and JCS exercises, is a rich opportunity to gather data, but also has inherent tensions and could possibly compromise the mission, especially if building relationships and trust between teams is essential to mission success.[48] This concern was echoed by an Army Special Forces Officers who was deployed in Iraq three times between 2005 and 2008. He noted that his team gathered biometric data on all FID partners in Iraq, but he expressed concern over insisting on gathering biometrics with JCETS. He noted, in particular, that collecting biometrics on JCETS with which U.S. forces have had a longstanding relationship would probably be construed as a violation of trust. He stated that, in situations like these, biometric collection would not be worth potentially damaging the relationship between teams.[49]

Context Four: Biometrics and Visitors to the United States

[45] "Interview with an Army Officer deployed to Afghanistan in 2009," interview conducted on August 5, 2010.
[46] "Interview with a biometrics expert in USSOCOM," interview conducted on July 27, 2010.
[47] "Interview with a biometrics expert in USSOCOM," interview conducted on July 27, 2010; and "Interview with a biometrics expert in SOCCENT," interview conducted on July 28, 2010.
[48] "Interview with a biometrics expert in SOCCENT," interview conducted on July 28, 2010.
[49] "Interview with an Army Special Forces Officer deployed to Iraq from 2005-2008," interview conducted August 11, 2010.

In response to the September 11th terrorist attacks on New York and Washington, the Department of Homeland Security (DHS) was created to "prevent and deter terrorist attacks and protect against and respond to threats and hazards to the Nation."[50] As part of that effort, DHS stood up US-Visit in 2004 to "to protect our nation by providing biometric identification services to federal, state and local government decision makers to help them accurately identify the people they encounter and determine whether those people pose a risk to the United States."[51] The primary means by which US-Visit gathers biometric information is through international visitors to the United States, including tourists, business travelers and, more recently, permanent foreign residents (Green Card holders).[52]

US-Visit's mission differs from DOD efforts at biometric collection in several important ways. US-Visit treats visitors to the United States as "non-derogatory," meaning that they are not assumed to be criminals or have mal-intent. US-Visit adheres to U.S. Privacy Laws for all individuals enrolled in the system and their personal data, despite the fact that the individuals are not U.S. citizens. US-Visit has also made public relations and transparency one of its key components, launching information campaigns around the world to explain why the data is being gathered, how it is being managed and protected, and who gets to see it. Finally, US-Visit has instituted a redress program, which allows individuals who feel they have been wrongly categorized to petition to change their status.[53]

The call to create US-Visit initially raised concerns with several constituents in the United States. The tourist industry was worried that the program would deter visitors to the United States and biometrics would slow down the immigration process. Privacy advocates and civil liberties groups were also concerned that information would not be managed and protected against theft and misuse. To abate these concerns, US-Visit brought stakeholders into the process, allowing them to raise concerns and offer input. A privacy expert in US-Visit noted, by way of example, that the original launch date of US-Visit was December 31, 2003. Travel and tourism groups voiced concerns about starting the program on a major travel day. US-Visit delayed the launch of the program to assuage these concerns. He also noted that civil liberties groups were concerned about racial profiling. To prevent that, US-Visit made it policy to gather data on everyone.[54]

The creation of US-Visit also raised concerns internationally. The European Union initially expressed concerns about privacy issues and management of data but, following the launch of the program, the European Union has adopted technology and policies similar to the United States.[55] Chile and Brazil also reacted negatively to the

[50] "One Team, One Mission, Securing Our Homeland: US Department of Homeland Security Strategic Plan, Fiscal Years 2008-2013," p. 3, available at, http://www.dhs.gov/xlibrary/assets/DHS_StratPlan_FINAL_spread.pdf, as of August 25, 2010.
[51] "DHS/ US-Visit," *Department of Homeland Security Website*, available at, http://www.dhs.gov/files/programs/usv.shtm, as of August 25, 2010.
[52] "Interview with three biometric experts at US-Visit," interview conducted on August 19, 2010.
[53] "Interview with three biometric experts at US-Visit," interview conducted on August 19, 2010; and "Interview with a privacy expert at US-Visit," interview conducted on August 19, 2010.
[54] "Interview with a privacy expert at US-Visit," interview conducted on August 19, 2010.
[55] "Interview with three biometric experts at US-Visit," interview conducted on August 19, 2010.

launch of the program. Brazil began requiring that all U.S. entering the country be fingerprinted as an act of reciprocity. The U.S. government responded by offering to help Brazil in its efforts to gather data.[56]

Individual travelers have had some concerns as well. US-Visit's privacy expert noted that fingerprinting is often associated with criminal activity; efforts were made to mitigate these perceptions, such as calling the process "finger scanning." Some expressed concern over health issues and the cleanliness of the equipment, particularly after the SARS and H1N1 outbreaks. US-Visit provided sanitizing wipes for individuals to manage these concerns. US-Visit also learned that U.S. citizens needed to be better educated on the immigration process and that they could provide a means of mitigating concerns of family members and friends visiting the country from foreign countries.[57]

Following the launch of the program, US-Visit conducted a privacy impact statement to measure compliance and resistance. Interviewees at US-Visit asserted that the program has been a success, both in its mission, and in mitigating concerns from countries and individuals about their safety and privacy. A privacy expert at US-Visit stated that he believed that the success of the program was the information campaign they executed prior to launching the program; that they have held the highest standards of the law and have had one set of rules for all; and that they have maintained transparency on the collection and management of the data. All of these efforts have created confidence and trust in the system.[58]

Findings

The four contexts described above yield some important findings for the use of biometric technology in future deployments for the U.S. military. These findings are divided into four categories: culture and biometrics; information operations; training; and data management.

Culture and Biometrics

The interviews suggest that culture is rarely an obstacle for biometric data gathering in combat environments, especially when incentives are tied to the process. Jobs and ID badges were particularly useful incentives in Iraq, and connecting biometric data gathering to healthcare in Afghanistan has also been a useful means of gaining the population's compliance. Even in conditions where little or no incentives were offered, such as efforts to collect biometrics on entire cities, culture was not a significant barrier for troops collecting data.

Tying biometrics to incentives does, however, have certain risks. Connecting biometrics to basic needs—such as food, water, and healthcare—may be unethical and possibly conflict with laws that govern the protection of civilians under occupation.

[56] "Interview with a privacy expert at US-Visit," interview conducted on August 19, 2010.
[57] "Interview with three biometric experts at US-Visit," interview conducted on August 19, 2010; and "Interview with a privacy expert at US-Visit," interview conducted on August 19, 2010.
[58] "Interview with a privacy expert at US-Visit," interview conducted on August 19, 2010.

Moreover, healthcare clinics may attract individuals that are low risk for insurgent activity, such as the elderly and women. Collecting their biometric data, in other words, may not be useful for tracking nefarious individuals. Similarly, tying biometrics to jobs and ID badges may also discourage insurgents from laying down their weapons and rejoining society because biometric data may connect them to past crimes.

Furthermore, in the short run, collecting biometric information on populations in conflict zones may have few cultural barriers. However, over the long haul, this dynamic may change. The Army Special Forces officer interviewed noted that gathering biometrics on other militaries as part of JCETs runs the risk of violating trust and compromising longstanding relationships.[59] The Army officer deployed to Afghanistan in 2009 echoed concerns of trust and damaging relationships through batting the Afghan National Army in his area of operation.[60]

In future conventional operations, one possible means of systematically gathering biometric data on the entire population may be through instituting a national identity card and connecting that card to various incentives that would ensure universal or near universal compliance. Future operations should also consider creating a redress program, similar to US-Visit's, as an important means of reassuring low level insurgents that they can opt out of fighting and become full members of society again. Using biometrics in this way would require planning, training forces, equipment and sufficient manpower devoted to this mission. As described by officers who attempted to enroll villages and urban centers in the HIIDE/Bats system, systematically gathering biometrics on large numbers of people at once cannot be accomplished without sufficient resources and planning.[61]

Information Operations Campaign

The interviews with experts at US-Visit point to the importance of a good public relations campaign to explain biometrics and their purpose. The logic behind informing the public on the purpose of biometric data gathering is to increase cooperation and compliance. Several officers interviewed noted that they explained to individuals, tribal leaders and groups that the biometrics data they were gathering was to help identify and catch insurgents and criminals. In these cases, this information aided their collection, rather than hindered it. Several officers also noted that, once they explained the purpose of biometrics to local police, the police would allow them to collect biometric information on individuals they had arrested.[62] Explaining the purpose of biometric data

[59] "Interview with an Army Special Forces Officer deployed to Iraq from 2005-2008," interview conducted August 11, 2010.
[60] "Interview with an Army Officer deployed to Afghanistan in 2009," interview conducted on August 5, 2010.
[61] "Interview with Marine Officer deployed to Anbar from 2007 to 2008, and 2009," interview conducted on August 4, 2010; "Interview with a Marine Officer deployed to Iraq in 2008 and Afghanistan from 2009 to 2010," interview conducted on August 6, 2010; "Interview with a Marine Officer in Afghanistan from 2009 to 2010," interview conducted on August 9, 2010.
[62] "Interview with Marine Officer deployed to Anbar from 2007 to 2008, and 2009," interview conducted on August 4, 2010; "Interview with a Marine Officer deployed to Iraq in 2008 and Afghanistan from 2009 to 2010," interview conducted on August 6, 2010.

gathering, in other words, may help assuage cultural constraints and encourage participation.

As with combat operations, information operations require forethought and planning. If biometrics are going to be an integral part of future U.S. military operations, then an IO campaign should be planned and integrated prior to deploying in order to increase the chances of mission success.

Training and Buy In

Most of the officers interviewed noted that they received limited to no formal training on how to use the HIIDE/Bats system. Several stated that the actual operation of the equipment was almost self explanatory and did not require much if any training. However, two officers noted that he and his team did not receive adequate instruction on the bigger purpose of biometric data gathering and its importance, or even whom they should be batting. The lack of explanation on the greater purpose of biometrics hindered interest in gathering the data.[63] The absence of education on the greater purpose of biometrics and whom to gather data on most likely created uneven collection across different areas of operation and within different commands.

A Marine officer deployed to Afghanistan from 2009-2010 also noted that there was little "buy in" to the importance of biometric data gathering within his unit's leadership. This was possibly due to the fact that his area of operation was semi-permissive and had a full mission set; biometrics, therefore, fell to the bottom of the list. Another possibility is that the leadership was not fully informed on the greater purpose of biometric data gathering and therefore they did not understand its potential. The same Marine noted that, without leadership buy in, biometrics "died on the vine."[64]

Data Coding and Management

Although this topic does not relate directly to the question of culture and biometric data gathering, the importance of data collection and management came up at several points during research. One Marine Officer noted that entire neighborhoods appeared to have been coded as detainees following the 2004 offensives in Fallujah, which created problems for vetting individuals down the road. His comments also suggested that, in addition to coding, tiers of biometric data were not used early on in the system to distinguish between citizens and criminals or insurgents.

A privacy expert at US-Visit noted that how the data is gathered matters for clarity and integrity, but how the data is coded matters even more; it needs to be compartmentalized and tiered in order to protect the rights of individuals in the system. Coding and managing the data are also tied to training and specialized personnel. Several

[63] "Interview with an Army Officer deployed to Afghanistan in 2009," interview conducted on August 5, 2010; "Interview with an Army Officer deployed to Iraq from 2006 to 2007," interview conducted on August 11, 2010.
[64] "Interview with a Marine Officer in Afghanistan from 2009 to 2010," interview conducted on August 9, 2010.

officers described that they worked with biometrics contractors who managed data they collected. One officer stated that he had a good working relationship with his contractor (who was a former Marine)[65] but nearly all other officers noted a difficult working relationship with contractors who managed the data they gathered in the field. Taken together, the gathering and management of biometric data in Iraq and Afghanistan appears to have been uneven.

The privacy expert at US-Visit also stated that why the data is being collected matters for coding. It appears that the U.S. military began using biometrics to gather information on detainees, but then moved to gathering data on the general population. The privacy expert asserted that data needs to be compartmentalized and tiered in a logical and consistent fashion—and, in particular, that average citizens need to be separated from criminals—in order for data to be shared between departments and agencies.

The biometrics expert at DBIDS echoed these requirements. He noted that the DBIDS system collects biometric data on U.S. nationals (contractors who work on bases overseas, for example) as well as foreign nationals. These categories are kept separate in the database, and only the data on foreign nationals goes up to BIMA.[66] Furthermore, data in DBIDS is tiered according to those who are entitled to gain access to the base under heightened security conditions.

Future use of biometric data collection in U.S. military operations would benefit from getting the right contractors forward deployed, better training with contractors and U.S. troops, and possibly more consistent coding of the data.

Cultural Questions for Using Biometric Technology in DOD Operations

Based on the findings of this research, below is a list of questions that the U.S. military could investigate prior to deploying to a region in order to gain a better understanding of the population's willingness to comply with biometric data collection.

1. What does the population know about biometric technology?
    a. From where is it learning about biometric technology?

2. Is the population's attitude towards biometric technology negative or positive?

3. Does the population have an identity card system? If so, what is their attitude towards it?

4. What is the population's expectations and rights surrounding privacy and civil liberties?
    a. Are there advocacy groups that promote civil liberties and the right to privacy?

[65] "Interview with a Marine Officer deployed to Iraq in 2008 and Afghanistan from 2009 to 2010," interview conducted on August 6, 2010.
[66] "Interview with a biometrics expert at DBIDS," interview conducted on August 6, 2010.

5. Does the population have a recent history of persecution by police forces or other domestic agents?

6. What are the threats facing the population? (eg. Terrorism, organized crime, refugee status)
    a. Can biometric technology help assuage these threats?

7. What incentives might promote voluntary cooperation with biometric data gathering?

8. Does the DOD have a public relations campaign to explain why biometric data is being gathered?

This page is intentionally blank

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Michael T. Yura
   International Biometrics Group
   and
   Biometrics Identity Management Agency

4. David Phares
   Biometrics Identity Management Agency
   Arlington, VA

5. Mike Elder
   Biometrics Identity Management Agency
   Arlington, VA

6. Gregory Alexander
   OSD

7. Paul C. Clark
   Naval Postgraduate School

8. Heather S. Gregg
   Naval Postgraduate School

9. Cynthia E. Irvine
   Naval Postgraduate School

10. Brian Greenshields
    Naval Postgraduate School

11. Gordon McCormick
    Naval Postgraduate School

12. Gregory Wilson
    Naval Postgraduate School