2010-12

# Biometric borders and counterterrorism

Moore, Todd M.

Monterey, California. Naval Postgraduate School


# NAVAL POSTGRADUATE SCHOOL

**MONTEREY, CALIFORNIA**

# THESIS

**BIOMETRIC BORDERS AND COUNTERTERRORISM**

by

Todd M. Moore

December 2010

Thesis Advisor: Maria Rasmussen
Second Reader: Ted Lewis

**Approved for public release; distribution is unlimited**

THIS PAGE INTENTIONALLY LEFT BLANK

| REPORT DOCUMENTATION PAGE | | | Form Approved OMB No. 0704-0188 |
|---|---|---|---|
| Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503. | | | |
| **1. AGENCY USE ONLY** *(Leave blank)* | **2. REPORT DATE** December 2010 | **3. REPORT TYPE AND DATES COVERED** Master's Thesis | |
| **4. TITLE AND SUBTITLE** Biometric Borders and Counterterrorism | | **5. FUNDING NUMBERS** | |
| **6. AUTHOR(S)** Todd M. Moore | | | |
| **7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)** Naval Postgraduate School Monterey, CA 93943-5000 | | **8. PERFORMING ORGANIZATION REPORT NUMBER** | |
| **9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)** N/A | | **10. SPONSORING/MONITORING AGENCY REPORT NUMBER** | |
| **11. SUPPLEMENTARY NOTES** The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number _____. | | | |
| **12a. DISTRIBUTION / AVAILABILITY STATEMENT** Approved for public release; distribution is unlimited | | **12b. DISTRIBUTION CODE** | |

**13. ABSTRACT (maximum 200 words)**

This thesis investigates the ties between biometrics and state security by analyzing biometric identification and screening programs, their structural elements, and ultimately their effectiveness. Although biometric identification is rapidly becoming an international norm, quantitative assessments of biometric identification programs within the larger context of state and international security are non–existent. This thesis discusses the idea of identity, defines the identity problem, addresses identity's role in state security, and addresses how biometric identification contributes to this end. Individual characteristics of the most prominently used biometric identifiers are discussed in detail (face, fingerprint, and iris), as well as the overall concept of biometric identification. The ICAO e–Passport program and the U.S. specific screening functions are presented to illuminate how biometric identifiers are used in practical applications. These programs, in turn, serve as the basis for the investigation of the effectiveness of biometric identification as it pertains to state security, focusing first on U.S. immigration and then on the broader context of international terrorism.

Biometric identification has been largely credited with producing tangible security gains. This thesis seeks to tie a quantitative measure to that assertion and generate future discussion about the merits of biometrically based identification and screening.

| **14. SUBJECT TERMS** Biometrics, Border Control, Counterterrorism, Immigration | | | **15. NUMBER OF PAGES** 149 |
|---|---|---|---|
| | | | **16. PRICE CODE** |
| **17. SECURITY CLASSIFICATION OF REPORT** Unclassified | **18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified | **19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified | **20. LIMITATION OF ABSTRACT** UU |

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

THIS PAGE INTENTIONALLY LEFT BLANK

**Approved for public release; distribution is unlimited**

**BIOMETRIC BORDERS AND COUNTERTERRORISM**

Todd M. Moore
Major, United States Air Force
B.S., United States Air Force Academy, 1996

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES**
**(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL**
**December 2010**

Author: Todd M. Moore

Approved by: Dr. Maria Rasmussen
Thesis Advisor

Dr. Ted Lewis
Second Reader

Dr. Harold A. Trinkunas
Chairman, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

# ABSTRACT

This thesis investigates the ties between biometrics and state security by analyzing biometric identification and screening programs, their structural elements, and ultimately their effectiveness. Although biometric identification is rapidly becoming an international norm, quantitative assessments of biometric identification programs within the larger context of state and international security are non–existent. This thesis discusses the idea of identity, defines the identity problem, addresses identity's role in state security, and addresses how biometric identification contributes to this end. Individual characteristics of the most prominently used biometric identifiers are discussed in detail (face, fingerprint, and iris), as well as the overall concept of biometric identification. The ICAO e–Passport program and the U.S. specific screening functions are presented to illuminate how biometric identifiers are used in practical applications. These programs, in turn, serve as the basis for the investigation of the effectiveness of biometric identification as it pertains to state security, focusing first on U.S. immigration and then on the broader context of international terrorism.

Biometric identification has been largely credited with producing tangible security gains. This thesis seeks to tie a quantitative measure to that assertion and generate future discussion about the merits of biometrically based identification and screening.

THIS PAGE INTENTIONALLY LEFT BLANK

# TABLE OF CONTENTS


I. BIOMETRIC BORDERS AND COUNTERTERRORISM ..... 1
A. WHY BIOMETRIC SCREENING ..... 1
B. PROBLEMS AND HYPOTHESES ..... 2
C. BIOMETRIC SCREENING IN CURRENT LITERATURE ..... 4
1. Identity ..... 5
2. Biometric Origins ..... 6
3. Biometric Screening ..... 6
4. Deterring Terrorism ..... 8
D. METRICS TO ASSESS BIOMETRIC BORDERS ..... 9
E. THESIS OVERVIEW ..... 12

II. BIOMETRICS AND IDENTIFICATION ..... 13
A. DISCERNING VERIFIABLE IDENTITY ..... 13
1. The Identity Problem Defined ..... 14
*a. Identification ..... 15*
*b. Authentication ..... 17*
*c. Authorization ..... 18*
2. Vulnerabilities of Identity Solutions ..... 19
B. BIOMETRIC SOLUTIONS ..... 20
1. Biometric Basics ..... 21
*a. Facial Photos ..... 22*
*b. Fingerprints ..... 24*
*c. Iris Scan ..... 26*
2. Using Biometric Identifiers ..... 27
*a. Templates of Identifiers ..... 28*
*b. Comparisons and Matching ..... 32*
*c. Recognition and Error Rates ..... 33*
3. Biometric System Components and Structure ..... 36
*a. Typical Program Components ..... 37*
*b. Biometric Database ..... 40*
*c. Biometric Vulnerabilities ..... 41*

III. BIOMETRIC BORDER CONTROLS ..... 43
A. THE PROCESS OF CROSSING BORDERS ..... 44
1. Immigration Background ..... 45
2. Immigration Process ..... 48
*a. Passport—Visa—Border ..... 48*
*b. Improving Identification–Authentication–Tracking ..... 49*
B. BIOMETRICS IN IMMIGRATION ..... 51
1. e-Passport Program—Solving Identification ..... 52
*a. Program Description ..... 52*
*b. Identifiers Used ..... 53*
*c. Identity Solutions ..... 54*

2. US–VISIT Program—Improving Screening ..... 56
*a. Origins of U.S. Screening* ..... *58*
*b. U.S. Screening Under HSPD–6* ..... *61*
3. U.S. Visa and Immigration Refusals ..... 63

IV. ASSESSING BIOMETRIC BORDERS ..... 73
A. BIOMETRIC SCREENING ..... 74
1. Defining Biometric Screening Periods ..... 76
2. Creating Standardized Database Information ..... 78
3. Identifying the Population of Interest ..... 81
B. AGGREGATE ANALYSIS ..... 86
1. Unknown/Other Included Dataset ..... 86
2. Unknown/Other Excluded Dataset ..... 89
C. GRAPHICAL ANALYSIS ..... 91
1. 1998—Malaysia ..... 92
2. 2004—Pakistan and Belgium ..... 94
3. 2005—Australia, Germany, New Zealand, Norway, Sweden, Thailand ..... 97
4. 2006—Austria, Denmark, France, Japan, Portugal, Singapore, UK, U.S. ..... 103
5. Overall Trends ..... 106
D. CORRELATION ANALYSIS ..... 108
1. Biometric Screening to Decreases in Terrorist Incidents ..... 109
2. Coding Dataset ..... 109
3. Correlation Outliers ..... 111
E. RESULTS ..... 112

V. CONCLUSIONS ..... 115
A. BIOMETRICS IN VERIFABLE IDENTITY ..... 115
B. ASSESSMENT RESULTS ..... 116
1. Screening Effectiveness ..... 116
2. Biometric Borders Vs. Terrorism ..... 117
3. Follow-on Research ..... 117
C. RECOMMENDATIONS ..... 118

LIST OF REFERENCES ..... 121

INITIAL DISTRIBUTION LIST ..... 131

# LIST OF FIGURES


Figure 1. Pre HSPD–6 Terrorist Watchlist Connectivity Diagram. ....60
Figure 2. Terrorist Identification and Watch Listing Under HSPD–6. ....62
Figure 3. U.S. Visa Ineligibles for Security and Terrorist Concerns. ....66
Figure 4. Terrorism and Security Refusal Trend Line. ....68
Figure 5. INA Security and Terrorism Refusal Percentages. ....69
Figure 6. Biometric Screening—1998 Start Date. ....92
Figure 7. Biometric Screening—2004 Start Date. ....94
Figure 8. Biometric Screening—2005 Start Date. ....97
Figure 9. Biometric Screening—2006 Start Date. ....103
Figure 10. Entire GTD Dataset—All Terrorist Activities (1971–2009). ....107

THIS PAGE INTENTIONALLY LEFT BLANK

# LIST OF TABLES


Table 1. Desired Characteristics of Human Identity Tokens. ....16
Table 2. Size Conversion of Digital Biometric Identifiers ....31
Table 3. Types of Errors in Immigration and Border Control ....34
Table 4. Error Rates of Biometric Matching Systems ....35
Table 5. ICAO Proposed Applications for Biometric Solutions....55
Table 6. Date Biometric Screening Established....75
Table 7. Raw Database Events by State of Interest. ....80
Table 8. Attack Type Events Committed by "Unknown/Other" Perpetrators. ....84
Table 9. Dataset Creation and Labeling. ....85
Table 10. Terrorist Incidents per Year (Unknown/Other Included). ....87
Table 11. Terrorist Incidents per Year (Unknown/Other Excluded). ....90
Table 12. Correlations of Screening to Annual Terrorist Incidents. ....110

THIS PAGE INTENTIONALLY LEFT BLANK

# LIST OF ACRONYMS AND ABBREVIATIONS

| | |
|---|---|
| AFIS | Automated Fingerprint Identification System |
| CA | Consular Affairs |
| DHS | U.S. Department of Homeland Security |
| DoD | U.S. Department of Defense |
| DOJ | U.S. Department of Justice |
| DOS | U.S. Department of State |
| EU | European Union |
| EURODAC | European Dactyloscopy |
| FRR | False Rejection Rate |
| FAR | False Accept Rate |
| IAFIS | Integrated Automated Fingerprint Identification System |
| ICAO | International Civil Aeronautics Organization |
| INTERPOL | International Criminal Police Organization |
| MRTD | Machine Readable Travel Document |
| SIS | Schengen Information System |
| US–VISIT | U.S. Visitor and Immigration Status Indicator Technology |

THIS PAGE INTENTIONALLY LEFT BLANK

# ACKNOWLEDGMENTS

I would like to acknowledge the dedication and professionalism of the instructors in the NSA department who daily endeavor to impart experience and wisdom. Thank you for your contributions to our academic endeavors and further expanding our critical thinking skills.

THIS PAGE INTENTIONALLY LEFT BLANK

# I. BIOMETRIC BORDERS AND COUNTERTERRORISM

This thesis will provide some background and insight on the rapidly developing biometric screening initiatives currently being adopted by several states in an attempt to counter terrorism within state borders. It will also attempt to assess the effectiveness of the biometric screening process by analyzing changes in terrorist activity by foreign nationals within nations that have instituted biometric screening programs to preemptively identify and stop individuals who may pose a security or terrorist threat. The intent will be to evaluate the effectiveness of biometric screening at national borders in countering terrorist activity by quantifying and comparing terrorist activity conducted by foreign nationals within select states as reported in the Global Terrorist Database (GTD.)[1] Using these incidents in conjunction with data on selected biometric identification and screening programs, I will attempt to determine if there exists a correlation between the advent of state biometric programs and the frequency of terrorist incidents. Throughout this thesis, relevant biometric programs will be explained and evaluated and the implications for biometrically based programs will be explored.

## A. WHY BIOMETRIC SCREENING

Biometric identification techniques have been increasingly incorporated into national security and immigration programs with the intent of improving the screening process and serving as a verifiable identity check at national borders. Many nations now incorporate biometric identification and authentication to screen and protect their populace from immigrants with the propensity to conduct criminal or terrorist activities. Biometric screening techniques may eliminate a dubious avenue that terrorists have used to access state borders by reducing an immigrant's ability to falsify or forge an identity. Developing a method to assess the utility of biometric identification and screening with respect to immigration and border security programs will further this area of research.

[1] The GTD is a product of: START - A Center of Excellence of the U.S. Department of Homeland Security, "Global Terrorism Database," University of Maryland, http://www.start.umd.edu/gtd (accessed 01 December 2009).

## B. PROBLEMS AND HYPOTHESES

The ability to positively identify individuals is rapidly becoming a requirement in light of increased personal mobility within broader global communities. Terrorists and criminals alike rely on the ability to remain unknown in order to carry out their nefarious activities. These individuals often go to great lengths to conceal or falsify their identity by using multiple aliases to cover up past events and often provide false information concerning portions of their identity.[2] Biometric identification is perhaps the best method to protect against identity falsification by conclusively identifying individuals based on their own unique physical properties.

Verifiable identity allows states to ensure security and accountability despite transient populations, essentially by threat of holding "individuals accountable for their actions."[3] As reported in 2004, there were over 27 different nations implementing biometric identification and border screening programs.[4] Since then, both common internationally recognized biometric screening programs and local variants are being rapidly expanded in several states. International standardization is being provided by programs such as *e–Passport,* which provides the required technology, integration and standardization initiatives to facilitate biometric programs. The e-Passport program is an International Civil Aviation Organization (ICAO) effort to implement machine readable visas (commonly known as passports) that can take advantage of "biometrics and their potential to enhance identity confirmation with passports."[5] The goal of e-Passport is to set universal requirements and standardization for "biometrically-enabled and globally-

---

[2] The 9/11 terrorists are a prime example of a group that used fictitious names to gain entry to the U.S., apparently a well-known terrorist tactic even before the 9/11 attack, see Thomas R. Eldridge, *9/11 and Terrorist Travel Staff Report of the National Commission on Terrorist Attacks upon the United States* (Washington, DC: National Commission on Terrorist Attacks upon the United States, 2004), http://purl.access.gpo.gov/GPO/LPS53197.

[3] Kristin M. Lord, *The Perils and Promise of Global Transparency: Why the Information Revolution may Not Lead to Security, Democracy, Or Peace* (Albany: State University of New York Press, 2006).

[4] C. Maxine Most, "Biometrics and Border Control: Beyond US-VISIT," *Digital ID World* (2004), http://magazine.digitalidworld.com/Sep04/Page18.pdf (accessed 04 March 2010).

[5] International Civil Aviation Organization, *Machine Readable Travel Documents: Specifications for Electronically Enabled Passports with Biometric Identification Capability*, 6th ed., Vol. 2, Doc 9303 (Québec, Canada: ICAO Secretary General, 2006) (accessed 09 October 2009).

interoperable passports." Currently there are over 61 states participating in this program.[6] In addition to internationally standardized programs, individual states are pursuing more localized biometric programs to include identification cards, border access cards and even programs that attempt to integrate civil and international criminal systems.

The biometric recognition market in the U.S. alone is projected to consume $5.7 billion in 2010, and most argue that the efficient use of developing biometric technology with respect to counterterrorism will greatly enhance immigration and border security.[7] State specific programs supplement the e–Passport system and provide enhanced screening based on biometric identifiers. The US–VISIT program (United States Visitor Indicator Status and Identification Technology) run by the U.S. Department of Homeland Security (DHS) is one of several state run biometric initiatives that actively gathers and utilizes biometric information to identify and screen immigrants.[8] Similar programs are in use in other states and biometric information is beginning to trickle between state governments in an effort to enhance both border and internal security.

Positively and verifiably identifying individuals with the potential to conduct terrorist activity before they have an opportunity to gain entry to a state's border, is crucial to reduce or limit the instances of foreign sponsored terrorist activity within state borders. Historically, several agencies have worked diligently to compile information on individuals perceived as terrorist threats, yet, these often comprehensive activities suffer with respect to verifiable identification. The main problem in terrorist identification and screening is that the typical information contained in most terrorist watchlists has been based purely on nomenclature. Until recently, most agencies relied singularly on name recognition software to screen intending immigrants. Biometric identification eliminates

---

[6] Find Biometrics, "Over 60+ Countries Now Issuing ePassports," *Security Document World* Articles (2008), http://www.findbiometrics.com/articles/i/6390/ (accessed 04 June 2010).

[7] J. Ackleson, "Securing through Technology?"Smart Borders" After September 11th," *Knowledge and Policy; the International Journal of Knowledge Transfer and Utilization* 16, no. 1 (Spring 2003), 56.

[8] See U.S. Dept of Homeland Security, "US-VISIT Biometric Identification Services," U.S., http://www.dhs.gov/files/programs/gc_1208531081211.shtm (accessed 09 December 2009).

the dependency on nomenclature and provides instantly verifiable identification to agencies that choose to correlate information and validate immigrants.

The conventional wisdom and proposed hypothesis of this thesis is that instituting biometric screening processes in immigration services will directly support terrorist deterrence in that successful foreign national terrorist attacks within a country with "biometric borders" should decrease after the implementation of biometric identification programs such as e-Passport and enhanced screening initiatives such as US–VISIT.

## C. BIOMETRIC SCREENING IN CURRENT LITERATURE

There appears to be an ample amount of information concerning biometrics and identification in existing literature, especially relating to security, counterterrorism and the potential gains from verifiable identification. Despite the debated merits of biometric identification technology itself, however, there is a relative absence of works that attempt to document or quantify the effectiveness of implemented biometric screening programs. Existing works on biometrics and counterterrorism span the spectrum from technological breakthroughs and postulated merits of emerging biometric systems to the speculated civil rights and privacy infringements that could accompany state biometric systems.[9] This prominent range of printed and electronic media address identity, biometrics, terrorism, deterrence, and criminology yet none attempt to academically correlate and quantify the contributions of biometric screening to counterterrorism as a whole.

In order to establish the foundation for researching links between biometric identification and deterrence with respect to terrorism, it is necessary to investigate biometric identification technology, system implementation methodology and other related avenues that may reveal the potential to "biometrically" counter terrorism. There is substantial information concerning identity, biometrics, and their proposed use in the fields of criminology and counterterrorism but few quantitative studies on effectiveness. Aside from media and journalist reports that highlight individual successes, there is a

[9] Kirstie Ball and Frank Webster, *The Intensification of Surveillance: Crime, Terrorism and Warfare in the Information Age* (London: Pluto Press, 2003); Louise Amoore, "Biometric Borders: Governing Mobilities in the War on Terror," *Political Geography* 25, no. 3 (01 February 2006), 366.

relative lack of research that focuses on the specific methodology or process of investigating biometric border controls. This thesis will lay the foundation for the practical assessment of state biometric identification and screening programs by focusing on e–Passport and US–VISIT.

### 1. Identity

Literature on identity conveys that the need to positively identify individuals is rapidly becoming a requirement in light of increased personal mobility within broader global communities. Biometric identification is premised on the identification of individuals by their unique and individual physiological characteristics. Computers and digitization moved these techniques well beyond the manual analysis of fingerprints and sped the advent of electronic processing.[10] Many existing works detail how this enabled more accurate fingerprint collection, storage, and analysis. Other works detail how biometrics are used in digital facial recognition, palm readers, retinal scans, or even gait analysis.[11] The preponderance of biometric based literature in circulation concerns the premise of biometrics or explores new techniques surrounding the field. Few published works, if any attempt to analyze the biometric component of any of the screening systems currently used for immigration or border security. The few that address newly implemented biometric programs are somewhat constrained government publications containing limited analytical data, opinion based editorials speculating success or failures, or journalistic pieces detailing specific publicized cases. The following captures some of the important flows of information that can be garnered form the biometric literature that will be relevant to this thesis.

---

[10] Myra Gray, "Terrorism and New Biometrics Technologies," *Security Magazine* 45, no. 11 (01 November 2008), 80–81, http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=35372561&site=ehost-live&scope=site (accessed 20 October 2009).

[11] Hong Lin and Jain Anil, "Integrating Faces and Fingerprints for Personal Identification," *IEEE Transactions on Pattern Analysis and Machine Intelligence* 20, no. 12 (1998), http://www.cse.unr.edu/~bebis/CS790Q/PaperPresentations/FaceFingerprintFusion.pdf (accessed 10 November 2009).

## 2. Biometric Origins

From fingerprints used well before the 1950s to emerging facial recognition software, a few works capture some of the new ideas on how to best use biometric technology to secure our nation. There are ample sources that cover some of the first usable identity verification programs, mostly from a historical or fact based context. For example, Watner and Sobieck highlight the utility of the Federal Bureau of Investigation's (FBIs) Integrated Automatic Fingerprint Identification System (IAFIS), which contains over 500 million fingerprint images (the German equivalent contains 4.7 million names, 2.1 million fingerprints and 1.9 million photos.)[12] It is also commonly reported that several other nations such as China, Japan, Australia, the UK, and even the U.S. Department of Defense (DoD) actively construct biometric databases for use in national screening programs.[13] Although not fully developed or coordinated, the ability to rapidly recall, process and correlate stored biometric data using powerful computers will continue to improve with the advent of interconnected networks and the development of better techniques for "data mining."[14] The ability to integrate databases and quickly process biometric information will be crucial in harnessing identification material for screening immigrants and potentially for future investigations or prosecutions.

## 3. Biometric Screening

The inclusion of biometrics into the immigration and border screening process was primarily developed and implemented in the United States after the events of 9/11. At the time, the U.S. made a concerted effort to tighten security by initiating biometric

---

[12] Carl Watner and Wendy McElroy, *National Identification Systems: Essays in Opposition* (Jefferson, NC: McFarland & Co, 2004); S. M. Sobieck, "Democratic Responses to International Terrorism in Germany," *Contributions in Political Science.* 340 (1994), 43.

[13] Dept of Homeland Security, "Government Agencies using US-VISIT," U.S., http://www.dhs.gov/files/programs/gc_1214422497220.shtm (accessed 17 October 2009); John D. Woodward Jr., "Using Biometrics to Achieve Identity Dominance in the Global War on Terrorism," *Military Review* 85, no. 5 (Sep/Oct, 2005), 30, http://libproxy.nps.edu/login?url=http://proquest.umi.com/pqdweb?did=942160821&Fmt=7&clientId=11969&RQT=309&VName=PQD (accessed 05 November 2009).

[14] Won Kim, "On US Homeland Security and Database Technology," *Journal of Database Management* 16, no. 1 (Jan-Mar, 2005), 1 (accessed 20 October 2009).

screening at our borders, as well as improving the ability of entry/exit tracking for all those visiting or immigrating. The U.S. Department of State (DOS) and the Department of Homeland Security (DHS) are the two main agencies responsible for screening prospective U.S. immigrants, to include biometric screening at our national borders. Some of the most recent additions to biometric screening programs are the inclusion of full digital fingerprints, facial recognition software and streamlined database integration.[15] These identification methods have the potential to identify individuals known to pose a threat to the U.S. and subsequently deny their entry.

Several "biometric screening" programs are being adopted by states for border control and internal security.[16] Some states are even considering national ID cards with embedded biometric identifiers.[17] Unprecedented levels of interagency coordination and information sharing will be required for these programs to succeed, the US–VISIT program alone incorporates "over 20 databases" to successfully identify and screen participants.[18] National fingerprint databases such as the Schengen Information System (SIS) and the European Dactyloscopy (EURODAC) databases are pursuing the means to integrate and share all available information within the European Union and even with foreign partners.[19] This ability to access and search other databases to correlate data has already paid dividends in the UK by identifying and denying several intended immigrants with multiple visa applications.[20] Improving control of the immigration process through

---

[15] U.S. Dept of Homeland Security, *US-VISIT Biometric Identification Services*

[16] Anneliese Baldaccini, "Counter-Terrorism and the EU Strategy for Border Security: Framing Suspects with Biometric Documents and Databases," *European Journal of Migration and Law* 10, no. 1 (January 2008), 31 (accessed 22 October 2009).

[17] Ian Hosein, "Transforming Travel and Border Controls: Checkpoints in the Open Society," *Government Information Quarterly* 22, no. 4 (01 October 2005), 594-625, http://www.sciencedirect.com (accessed 20 October 2009); Martin J. Garvey and Eric Chabrow, "Border ID System First Part of $10B Effort," *Information Systems News*, no. 971 (12 January 2004), 22, http://www.informationweek.com/story/showArticle.jhtml?articleID=17300298 (accessed 09 October 2009).

[18] Amoore, *Biometric Borders: Governing Mobilities in the War on Terror*, 336.

[19] Baldaccini, *Counter-Terrorism and the EU Strategy for Border Security: Framing Suspects with Biometric Documents and Databases*, 31.

[20] M2 Presswire, "Ten Point Plan for Border Protection and Immigration Reform; First Milestone Met as Fingerprint Checks Go Global." *Normans Media Ltd*, sec. UK Government, 14 January 2008, http://proquest.umi.com/pqdweb?did=1412330111&Fmt=7&clientId=11969&RQT=309&VName=PQD (accessed 17 March 2010).

verifiable identify in the form of biometrics seems to be tightening immigration loopholes, which could otherwise be utilized by criminals and terrorists alike.

### 4. Deterring Terrorism

Actively deterring terror seems to be the driving force behind many government–sponsored programs aimed at increasing security, especially now that vulnerabilities have been exposed post--9/11.[21] Although deterrence remains at the forefront of many government objectives and many security experts claim "deterrence works," the ability to assess deterrence appears highly contested and very difficult to prove.[22] The inherent problem is the ability to ascertain acts that have not, do not, or will not happen. We may never know how many "attacks have been averted because of the measures the U.S. government has taken."[23] Without candid information on terrorist intentions, assessing terrorist deterrence seems to be a subjective assessment at best. Despite the difficulty detecting deterrence, variance in the number of successful terrorist incidents may still be a strong indicator of the relative performance of biometric screening.

Biometric capabilities and techniques in criminal identification are well documented; but again it appears very little academic research has focused on methodically exploring the effectiveness of biometric identification in countering terrorism. Perhaps due to the relative novelty of biometric screening, most works have only focused on the technological aspects of implementation and the documentation of specific instances of biometric use. Most of the current literature concerning biometric effectiveness is journalistic in nature and suffers from a lack of comprehensive statistical backing. Several of the works centered on biometric screening analysis emanate from

---

[21] John Frittelli, *Transportation Security: Issues for the 109th Congress* (Washington D.C: Congressional Research Service, Library of Congress, July 2005), http://fpc.state.gov/documents/organization/52533.pdf (accessed 15 May 2010).

[22] Bianca Bersani, Paul Nieuwbeerta, and John Laub, "Predicting Trajectories of Offending Over the Life Course: Findings from a Dutch Conviction Cohort," *The Journal of Research in Crime and Delinquency* 46, no. 4 (2009), 468; Bruce Schneier, *Beyond Fear: Thinking Sensibly about Security in an Uncertain World* (New York: Copernicus Books, 2003); David Bonner, "United Kingdom: The United Kingdom Response to Terrorism," *Terrorism and Political Violence* 4, no. 4 (1992), 171, http://www.informaworld.com/10.1080/09546559208427180 (accessed 23 October 2009).

[23] Kim, *On US Homeland Security and Database Technology*, 1.

media organizations and national governments and tend to reference specific or individualized successes or failures. Examples range from local newspapers reporting immigration offences in the UK, which were discovered using biometric screening, to government-sponsored reports on the effectiveness of the U.S. border screening programs, which contain very few statistical data points.[24] Other common works are often in editorial or opinion based format, such as the expose of the "20th hijacker" in the 9/11 plot.[25] It is apparent that the statistical data on biometric screening initiatives is of a somewhat sensitive nature that is not readily released as some U.S. authors have documented that their requests for data under the Freedom of Information Act are often met with resistance and fail to yield any real results.[26] Considering the relative youth of biometric screening and the difficulty in obtaining pertinent data, it is understandable that few works attempt to correlate biometric data in relation to identified terrorist activities.

## D. METRICS TO ASSESS BIOMETRIC BORDERS

In an effort to investigate and quantify the contributions of biometric identification and screening towards countering terrorism, this thesis will correlate, quantify and assess terrorist attacks with respect to the establishment of state biometric screening programs or "biometric borders." After explaining the current biometric identification programs and their components, this thesis will perform an analysis of U.S. immigration screening programs with respect to the incorporation of biometric information. Specifically, it will look at the changes in the number of intending U.S. immigrants denied entry due to security and/or terrorist related concerns by comparing U.S. visa refusals in the category of terrorism and security concerns again with respect to the incorporation of biometric screening programs into the immigration process.[27] The analysis will focus on the visa refusal categories that fall under the issues of security and

---

[24] Louis Chunovic, "Stopping Terrorist Travel: The Pre-Flight 253 View," *Government Security News* 8, no. 2 (01 Feburary, 2010), 1–23, www.gsnmagazine.com (accessed 05 March 2010).

[25] Woodward, *Using Biometrics to Achieve Identity Dominance in the Global War on Terrorism*, 30.

[26] David North, "At DHS, Perps have Rights that Citizens Don't," Center For Immigration Studies, http://www.cis.org/north/perps-have-rights (accessed 08 May 2010).

[27] U.S. Visa refusal statistics are tracked by the U.S. Dept of State and can be accessed at http://travel.state.gov/visa/frvi/statistics/statistics_1476.html.

terrorism as defined in the 1952 Immigration and Nationality Act.[28] Refusal figures in this category will be compared with respect to biometric implementation and also normalized over the number of immigrant applications in order to account for changes in immigration activity. One limitation in the refusals dataset is that no information is divulged on the purpose or basis for the visa refusal. This directly limits the ability to verify that biometrics played a role in the refusal process. Thus, while biometric information cannot be directly correlated to the refusal rates, it seems that an increase in the relative quantities refused may imply that the U.S. is increasing terrorist identification capabilities due to biometric screening, if there are no other intervening variables in the immigration process.

Building on this limited U.S. specific analysis, this thesis will move to analyze the first twenty states to implement biometric identification and screening policies. This larger scale analysis will take into account terrorist incidents conducted within a country by foreign nationals before and after implementation of a recognized biometric screening process in order to determine appreciable changes in the overall quantity of terrorist incidents with respect to biometric identification programs. The aggregate numerical analysis will be complimented by an investigative study of the correlations between biometric screening programs and decreases in terrorist incidents. The ultimate aim will be to combine the findings from the quantitative analysis of terrorist incidents with respect to biometric borders and the assessment of U.S. immigration screening effectiveness after the incorporation of biometric technology in an attempt to draw conclusions about the overall contributions of biometric screening to countering international terrorism.

The primary database for terrorist incidents will be the Global Terrorism Database (GTD) compiled by the National Consortium for the Study of Terrorism and Responses to Terrorism and published as an open-source product by the University of Maryland, which contains all terrorist incidents between 1991 and 2007.[29] The GTD dataset

---

[28] As per § 212(a)(3); 8 USC. § 1182(a).

[29] Available from: START - A Center of Excellence of the U.S. Department of Homeland Security, *Global Terrorism Database*.

contains global terrorist activity with over 80,000 attacks and provides the ability to classify individual incidents. Classifying the dataset by perpetrator nationality and target location will be the primary method used to identify foreign nationals conducting activity against a specific state. In order to isolate the screening process with respect to terrorist activity, incidents within the dataset will be qualified to only include events perpetrated by an individual subject to the screening process. These events will only include terrorist attacks against a state performed by a foreign national who would have been subject to immigration or border screening. Within this qualified dataset, events will be quantified and analyzed with respect to the implementation of biometric screening.

One expectation with the implementation of a biometric screening program is that there will be some instantaneous benefits from identity verification and other benefits that develop over the course of the program as database functions become more developed. Results will be assessed with the understanding that there may be some lag before results might be realized due to the intense reliance upon database creation, sharing, and integration as well as the associated systems being distributed and operated effectively. This thesis will focus on the implementation of biometric screening systems as a delineator to discern any changes in terrorist activity or U.S. visa refusals, but it will also consider that benefits from such systems should continue to improve with time.

Based on the nature and sensitivity of biometric screening information, few details that enable direct correlation with respect to terrorist attacks or visa refusals are released to the public. In light of this, it may not be possible to show a strong direct correlation between biometric screening and terrorist activity within a state or by analysis of the U.S. visa refusal rates, yet certainly these quantifiable measurements should lend some assessment of current biometric screening programs. Despite this, case studies and journalistic pieces that contain specific biometric screening successes or failures will continue to provide limited indicators of biometric performance. These instances will be addressed where appropriate.

Combining the quantitative analysis of terrorist incidents and visa refusal rates with respect to biometric screening with a program capabilities analysis and specific case studies should provide a comprehensive analysis of the merits of biometric screening.

With respect to immigration and border security, further research could provide much stronger correlation if similar analysis could be conducted at a level of fidelity where biometric screening information can be directly correlated with individual terrorist incidents or specific visa refusals.

## E. THESIS OVERVIEW

This thesis will be organized in a manner that will provide some background information on the topic of biometric identification, explain the specific programs currently in use for immigration and border security, then lead into the individual methods of analysis and ultimately draw conclusions from the results and provide recommendations for the future of biometric identification programs. Chapter II will introduce the issue of verifiable identity, address why it is required, define the specific identification problems, and introduce how biometrics contributes to this end. Although not intended to be a primer on biometrics in general, some detailed information on the field and related programs is necessary for the ensuing discussion in the following chapters. Chapter III discusses identity throughout the immigration process and illustrates how biometric identification and screening is being integrated through programs such as e–Passport and US–VISIT. It concludes with the analysis of the U.S. visa refusal rates as they relate to the U.S. biometric screening initiatives—essentially a small scale assessment of biometrics in immigration. Chapter IV then launches into a much larger scale study of terrorist incidents as they compare to specific state biometric programs. This chapter concludes with the results of this analysis and offers some suggestions for future analysis of "biometric borders." Finally, Chapter V ties together the capabilities of biometric identification in state security and border control by summarizing the results of the studies. Based on this analysis, recommendations are provided for current and future biometric initiatives as well as possible assessment methods. This section will also highlight the limitations of this thesis and provide recommendations for further research on the topic.

# II. BIOMETRICS AND IDENTIFICATION

The quest for verifiable identity is rapidly gaining momentum in today's increasingly globalized culture. In the wake of a perceptible increase in cross–border terrorist attacks, several states are turning to biometric identification programs for immigration screening and border control. States ultimately desire comprehensive border control systems capable of accurately identifying and then denying entry to an individual who may intend to inflict harm or conduct nefarious activities within their borders. Biometric identification programs focus on identity verification, authentication, and screening using unique human identifiers. These systems combine human characteristics with computers to positively ascertain then subsequently validate an individual's identity.

Biometric systems are continually expanding into state border control programs and many exert claims of measureable security gains as a result of this advanced technology. In order for states to quickly solve the identification and authentication problem, biometric identification systems must be carefully designed and implemented. They must also incorporate or access comprehensive biometric identity databases. This chapter will identify some of the problems with discerning individual identities and highlight the potential contributions of current biometric technology in relation to the immigration process.

## A. DISCERNING VERIFIABLE IDENTITY

For the context of this study, identification and identity will be used to describe the process of associating an identity with a specific individual, often termed *personal identity*.[30] In a social context, the ability to claim a unique and individual identity is the basis for relationships with other individuals, businesses, societal structures, and institutions. In this sense, a personal identity is considered a unique attribute of which a single individual person is the sole proprietor. In addition to physical identification, individual identities are rapidly becoming the basis by which an individual is verified and

[30] Anil K. Jain, Ruud Bolle and Sharath Pankanti, eds., *Biometrics: Personal Identification in Networked Society* (New York: Springer Science+Business Media Inc., 1996), 1.

potentially trusted.[31] The ability to develop basic social relationships, gain individual rights and services, and to a greater extent, functioning as cohesive society would be difficult to achieve without the ability to use our individual identities.[32]

Our cognitive and visual abilities have led humanity to "visually" verify the identity of those within their immediate familiar surroundings. Typically visual identification is based on physical features mainly through facial recognition or other distinguishable physical characteristics (height, hair color, eye color, structure.) Throughout the development of civilization, local knowledge of an individual's historical upbringings and close social intimacy within communal societies made this possible. When people began to interact outside the immediate bounds of their local societies, validating one's identity to other individuals became a necessity. Identifying and authenticating personal identities is necessary in order to convey trust and facilitate exchange. This increasing external interaction, outside the limited social circles in which we are able to be "visually" verified, has driven the demand for better methods of establishing verifiable identity.

### 1. The Identity Problem Defined

The question of verifying identity is widely viewed as a problem defined by two distinct issues—identification and authentication.[33] These identification problems are often centered on determining exactly who a person is and somehow verifying this information through a reliable mechanism. Jain et al., point out that the identification problem can often take on very different forms, from discerning an identity from a set of known identities to attempting to establish a new previously unknown identity. Solutions to the first part of the identity problem have historically been in the form of names, birthdates, signatures, photos, or other items that we consider to be personally unique to

[31] Stan Z. Li and others, eds., *Advances in Biometric Person Authentication: 5th Chinese Conference on Biometric Recognition, SINOBIOMETRICS 2004, Guangzhou, China, December 13–14, 2004, Proceedings* (Berlin, Germany: Springer, 2004), 1.

[32] Ruud M. Bolle and others, eds., *Guide to Biometrics* (New York: Springer, 2004), 3.

[33] Jain, Bolle and Pankanti, *Biometrics: Personal Identification in Networked Society*, 1–2.

an individual. The need to interact without being physically present as well as the ability to convey trust and assurance of your identity has necessitated other methods by which to verifiably identify individuals.

The second portion of the identity problem is identity authentication, more directly put this is the process of verifying the identification of an individual once their identity has been determined via an acceptable method. Again this problem can take various forms, from confirming a known identity to comparing an identity against a comprehensive list of other identities, or *screening*. Authentication solutions have traditionally been sought from either: something a person knows—*password*; or something a person has—*token*; but may soon be in the form of what a person is—*biometrics*.[34] Authentication can be used in a number of ways. Most often in border control it is used to confirm that an identity either is or is not in a set of known identities.

Solving the identity problem is a necessary first step in the immigration process especially as states look to protect their citizens from malevolent actors. Each portion of the identity problem can be critically important to immigration, identities need to be accurately created and a method needs to be in place that offers reliable authentication. Screening is becoming an integral to the immigration process in order to properly vet individuals and protect states. While many states often have similar methods for establishing identities (birth certificates or birth records) most have vastly different methods of authenticating identities (fingerprints, drivers license photos, national numbers, personal interviews, etc.) Looking at the components of the identity problem and how it specifically relates to immigration can illustrate the utility of biometrics in solving the identity problem and bolstering state security.

#### *a. Identification*

The basic premise of identification in immigration and border control is that each individual person can ultimately have a unique identity that can be readily presented and verified in order to receive the desired service. There are a range of

[34] Schneier, *Beyond Fear: Thinking Sensibly about Security in an Uncertain World*, 182–183.

possible human identifiers that could be used in this process, potentially even a combination of identifiers that when used in combination, contribute to determine an identity. Despite the identifier(s) used to represent an individual human identity, many researchers seem to agree with Roger Clarke that human identifier(s) must meet a stringent set of characteristics in order to fulfill the intended purpose of reliable identification.[35] The following table lists the criteria set forward by Clarke for use in determining the suitability of human identifiers.

**Desired Characteristics of Human Identity Tokens**

Richard Clarke (1994)

| Human Identifier Characteristic | Description |
|---|---|
| **Universality** | Every Relevant Person Should Have One |
| **Uniqueness** | No Two Persons Should Have the Same Identifier |
| **Permanence** | Should Not Change Over Time |
| **Indispensability** | Should be a Feature Intrinsic to the Person |
| **Collectability** | Able to be Collected by Anyone on Any Occasion |
| **Storability** | Storable in Manual and Automated Systems |
| **Exclusivity** | Able to be a Standalone Identifier |
| **Precision** | Sufficiently Different from Other Identifiers |
| **Simplicity** | Recording and Transmission Should be Simple |
| **Cost Effectiveness** | Measuring and Storing Should be Cost Effective |
| **Convenience** | Relatively Easy to Measuring and Storing |
| **Acceptability** | Conform to Contemporary Social Standards |

*Information adapted from Roger Clarke's 1994 article in *Information Technology and People* titled "Human Identification in Information Systems: Management Challenges and Public Policy Issues."

Table 1. Desired Characteristics of Human Identity Tokens.

Assessing the criteria for human identifiers, it seems apparent that a nomenclature or numerical based system for identification will quickly encounter problems in the areas of uniqueness and indispensability, not to mention the security of such a generic identifier when attempting to put it into use. It is also clear that more advanced and highly reliable methods of personal identification such as DNA (deoxyribonucleic acid) genotyping are clearly too cumbersome and would not pass the

[35] Roger Clarke, "Human Identification in Information Systems: Management Challenges and Public Policy Issues," *Information Technology and People* 7, no. 4 (1994), 6–37.

criteria for simplicity, convenience, cost effectiveness, or acceptability.[36] In order to comply with a majority of these criteria, human identification solutions today often rely on the inclusion of several different identifiers (photograph, name, birthday, social security number, address, hair or eye color, height, weight, etc.) Using biometric identifiers can offer significant improvements, particularly in the areas of uniqueness, permanence, exclusivity, and convenience. Taking all the criteria into account, it seems that using biometric identifiers can better address almost all of Clarke's desired characteristics of human identity tokens.

### *b. Authentication*

The second part of the identity problem is verifying the identity of an individual once a suitable identifier is presented or obtained. This has traditionally been based on the human ability to visually recognize individuals from photographs, or discern the accuracy of a password. These methods required an individual to know or posses some sort of information or item to validate their identity. Today, computer systems have increased the ability to repeatedly and accurately solve this part of the identity problem solely based on the individual's biometric characteristics.[37] As with traditional systems, there must be a method to first create the authentication devices and tokens and then a complimentary storage or database system capable of retaining and/or accessing the information in order to ensure valid authentication.[38] Authentication methods can involve multiple approaches and may still incorporate tokens and/or passwords to ultimately accomplish the objective. Although various methods can be combined to create different identification and authentication solutions using tokens and passwords, most traditional methods are subject to potential disruption via fraud, stolen or misplaced

---

[36] The characteristics of DNA (deoxyribonucleic acid) and its unique ability to verifiably identify an individual were first discovered in the 1980s in the UK. Howard Safir and Peter Reinharz, "DNA Testing: The Next Big Crime-Busting Breakthrough," *City Journal* Winter 2000, http://www.city-journal.org/html/10_1_dna_testing.html (accessed 15 May 2010).

[37] Stephen T. Kent and others, *IDs–Not that Easy: Questions about Nationwide Identity Systems* (Washington, D.C: National Academy Press, 2002), 34.

[38] Kim, *On US Homeland Security and Database Technology*, 1.

information, database disruption, security breaches, or identity theft. Biometrics offers substantial security improvements to authentication through the use of an individual's proprietary physical characteristics.

As mentioned earlier, authentication can be positive or negative depending on the application. Positive authentication is verifying that an individual is who they claim to be, while negative authentication is verifying that an individual is not some other known individual. The authentication process in immigration and border control is commonly referred to as *screening* and is becoming heavily reliant on biometric identification. Many states are now using comprehensive databases of known criminals or other "most wanted" types of individuals to accomplish effective screening at their borders. An example of biometric based authentication would be individuals presenting fingerprints at a border point of entry (POE) and that print being subsequently compared to all the others within a database of "most wanted" individuals. In this example, the individual is being *negatively authenticated* in that the agency or state is ensuring that he is not matched to any of the "most wanted" individuals.

#### *c. Authorization*

Some also add the term *authorization* into the identity problem. The use of authorization is meant to be the privilege, item, or service that a person is attempting to obtain as a result of providing verifiable identity. This addition is logical as usually the identity problem is being solved as part of a desire for the exchange of information or services. In today's globalized and highly interconnected environment; bank accounts, driver licenses, credit cards, online retailers, and even military installations all rely on various methods to identify and authenticate individuals in order to subsequently authorize a corresponding service. Familiarization with these terms and understanding the associated problems can help navigate discussions about identity based transactions despite each individual application.

### 2. Vulnerabilities of Identity Solutions

While most identity verification needs can be met using various solutions to these two identity problems—this system has some inherent weaknesses. First, establishing an identity is a difficult problem that can be subject to error if either falsely created at the outset or maliciously modified. Second, traditional methods of identification and authentication that make extensive use of tokens and passwords have a high potential for these items to be either stolen or used by "unauthorized" persons.[39] Finally, very few of these traditional identity systems have the ability to be commonly integrated for the purpose of screening individuals.[40] The existing vulnerabilities of the traditional solutions to the identity problem illuminate the need for a more secure, robust, and interoperable system capable of providing verifiable identity.

Subsequent to the 9/11 attacks, it has become increasingly clear how terrorist operatives have been able to circumvent several identify creation and verification procedures. These perpetrators, some already known terrorists at the time, were able to gain access into the U.S. through the immigration system by taking advantage of the multiple vulnerabilities within our identification and authentication systems. Beginning with establishing identities, the 9/11 commission reported that "the 19 hijackers used 364 aliases" to assist in gaining passports for travel to the US.[41] It was also discovered that two of the hijackers had obtained passports that were stolen from the Saudi Arabian embassy.[42] Two other hijackers gained entry to the U.S. with passports that contained fraudulent entry–exit stamps that were intended to hide travel to/from Afghanistan for terrorist training, illustrating how some well intended "tokens" can be used in a fraudulent manner.[43] Finally, three of the hijackers were known to U.S. intelligence, yet

---

[39] Jain, Bolle and Pankanti, *Biometrics: Personal Identification in Networked Society*, 3.

[40] Four years after the 9/11 attacks, several of the U.S. agencies failed to integrate or improve immigration screening capabilities. See: Thomas H. Kean and Lee Hamilton, *Report on the Status of 9/11 Commission Recommendations* (Washington, DC: 9/11 Public Discourse Project, 2005).

[41] Eldridge, *9/11 and Terrorist Travel Staff Report of the National Commission on Terrorist Attacks upon the United States*, 1.

[42] Ibid., 2.

[43] Ibid., 1.

were still able to successfully transit the U.S. border on multiple occasions. This was mainly due to the fact that U.S. systems were not able to capitalize on the intelligence information already obtained by government agents and contained in "the terrorist watchlist."[44] Ultimately, the hijackers were able to falsify the creation of their identities, leverage stolen or falsified passports, and circumvent U.S. screening systems. Looking at the 9/11 attack from the perspective of immigration and highlighting the areas where the perpetrators took advantage of the known vulnerabilities of the basic identity problem, it is apparent why the U.S. decided to address our immigration system and its traditional nomenclature based process of identity creation, authentication, and screening.

Before biometrics, a state's ability to establish individual identities and subsequently apply some type of screening process relied almost entirely on a nomenclature based system. Individuals are assigned names at birth and these nomenclature identifiers are subsequently built upon by various institutions throughout an individual's experience within the state infrastructure. Most of this process relies on the addition of other human identifiers or pieces of information determined to be unique to that individual. At the time that nomenclature was largely put into use, there were few if any systems that could credibly establish a quality baseline for the initial identification of an individual human identity. This system of nomenclature based identification is a substantial vulnerability in immigration and border control, but can be substantially improved by the addition and incorporation of biometric identification methods at an appropriate time within the identity formation and authentication process.

## B. BIOMETRIC SOLUTIONS

The ability to leverage our unique and highly individualized human characteristics in personal identification has long been practiced and is currently referred to as biometrics. Biometric identification is essentially the practice of using a "physiological or behavioral trait that may be measured and subsequently identified in order to confirm

[44] Eldridge, *9/11 and Terrorist Travel Staff Report of the National Commission on Terrorist Attacks upon the United States*, 68.

an individual's identity."[45] Through recent advances in computer technology and automation; the use of biometrics in human identification is now a very viable option. Biometric identification in immigration and border control is specifically aimed at reducing or eliminating the multiple vulnerabilities inherent in the identity system and enhancing the reliability of screening programs. The ability to digitally capture and quickly compare complex and unique human characteristics allows states to capitalize upon human characteristics for verifiable identity. The use of biometric identifiers is another tool that can be effectively used by state enforcement officials in nearly all security realms, including the current efforts of countering international terrorism.

Biometric identification has gained momentum in the last decade primarily due to advances in technology and procurement, which spurned subsequent security successes by state and international agencies. This section will illustrate the history of biometric identification, discuss some of the more common biometric identifiers used in criminal and immigration applications (facial photos, fingerprints, and iris scans) and show how biometric technology can substantially improve a state's ability to solve the problem of identification and authentication with respect to immigration and border control. Understanding the characteristics of these biometric identifiers, the underlying technology that enables collection and processing, and some of the challenges confronting their use in identification is a necessary first step in determining the potential applicability of biometrics in security applications.

### 1. Biometric Basics

Although the term biometrics is relatively new, the concept of using human characteristics to define and verify individual human identities originated early in human history.[46] The 20th century, however, can be credited with seeing the most profound developments in using biometrics for identification and security. Perhaps the first biometric tool to extend beyond the basic visual comparison method was fingerprint

[45] Julian Ashbourn, *Practical Biometrics: From Aspiration to Implementation* (London; New York: Springer, 2004), 1.

[46] Ibid., ix.

analysis, which has since provided unprecedented gains in criminal identification.[47] The subsequent integration of computer technology revolutionized biometrics by creating the ability to rapidly digitize, store, and compare individual identifiers. Recently the field and study of biometrics has exploded beyond fingerprints and facial photos and is experimenting with identifiers such as speech, gait, and even odor recognition.[48] In the continual quest for physically unique and highly reliable identifiers, researchers are looking towards the human iris, retinal wall, and even some highly detailed facial features. Biometric researchers continually demonstrate that all these individual features have unique characteristics capable of being electronically identified with unprecedented levels of accuracy and reliability.

The field of biometric identification is continually gaining ground as a viable alternative to the nomenclature based identity system upon which we previously relied to establish unique and credible identities. As states pursue biometric identification and screening options to supplement established programs, most states have decided to use the most commonly accepted and least intrusive biometric identifiers of facial photos and fingerprints. This has led to the creation of an international standard for biometric passports that includes facial photos, fingerprints, and iris scans.[49] The ability to properly use these highly unique and accurate identifiers certainly has the potential to improve the reliability and portability of identification solutions that are now mandated by the unprecedented levels of global human mobility and the accompanying increases of state border transits.

#### *a. Facial Photos*

While not commonly thought of as a biometric identifier, facial recognition is perhaps one of the most highly used and least intrusive identifiers available

[47] Jain, Bolle and Pankanti, *Biometrics: Personal Identification in Networked Society*, 44.

[48] Bolle and others, *Guide to Biometrics*, 55–59.

[49] International Civil Aviation Organization, *Machine Readable Travel Documents: Specifications for Electronically Enabled Passports with Biometric Identification Capability*.

to biometric applications today.[50] Since the inception of photography, facial photos have been incorporated into several identification and authentication schemes. The ability to use facial photographs for the purposes of identification stem from the unique human ability to rapidly compare a photograph to a live individual and assess the likeliness of a match with a relatively high degree of accuracy. States and organizations both make extensive use of facial photographs in many identification programs, typically superimposing or embedding images upon a token, which is given to the individual user. This method is a prominent identification scheme currently used in driver licenses, military ID cards, and passports.[51] The ability to digitize facial photos and store the information in a retrievable form (either in a central database or embedded within the token) has furthered the use of facial photographs as a potential identity screening mechanism. Incorporating computerized recognition technology to the natural patterns associated with facial photographs has proven a bit more difficult, but is yielding progress as computers, imaging equipment, and software continue to develop.

There are several methods currently available that attempt to automate facial recognition through the use of computer technology. These various methods range from manual mapping algorithms based upon a grid type of system to complicated infrared identification schemes that rely on the underlying structure of the blood vessels.[52] Although technology is proving that facial photographs can be a reliable biometric for authentication, they are also subject to problems in conditional lighting, facial expressions, capture device capabilities, and formatting; which makes this identifier somewhat troublesome for positive automated identification.[53] Understandably, the reliability of facial photos in identification goes significantly downwards as the visual or image acuity deteriorates. As such, facial photographs are better suited for use in a controlled environment and mainly for lower security applications. Despite some of these problems, consistent advances continue to be made

---

[50] Simson Garfinkel, *Database Nation: The Death of Privacy in the 21st Century* (Sebastopol, CA: O'Reilly, 2000), 55.

[51] Bolle and others, *Guide to Biometrics*, 36.

[52] Jain, Bolle and Pankanti, *Biometrics: Personal Identification in Networked Society*, 193–197.

[53] Ashbourn, *Practical Biometrics: From Aspiration to Implementation*, 22.

in the capturing, processing, and screening of facial photographs. Similarly, due to its non–invasive nature and quick ability to be discerned by human visual examination, facial photographs are proving to be one of the most universal biometric identifiers.

### *b. Fingerprints*

The advent of fingerprinting could be credited as being perhaps the most significant contribution towards verifiable identity and is becoming the hallmark of biometric identification. The human fingerprint has seen the longest and most consistent use as a highly reliable biometric identifier, and fingerprint technology has recently enjoyed some substantial improvements. The ability to capture, process, analyze, and share this biometric identifier has developed to the point that some programs are using fingerprints as a standalone identifier.[54] Considering these improvements in current technology, digital fingerprints are perhaps the best biometric identifier that can be effectively used for both establishing and authenticating an individual human identity.

Fingerprints are truly unique to an individual and nearly independent from our genetic makeup, making them an ideal biometric identifier.[55] Discerning differences between fingerprints is largely based on measuring the ridges and troughs found in the skin, commonly known as *minutiae*.[56] The unique designs made by the minutiae are classified according to their physical characteristic, which allows individual prints to be cataloged and compared. As the ability to collect, catalogue, and effectively analyze individual prints was perfected in the early 1900s, states and international organizations began collecting fingerprints and manually analyzing these remarkably unique and highly

[54] The U.S. Secure Communities Initiative is program designed specifically to cross–check inmate fingerprints with national immigration records in an effort to validate citizenship. Spencer S. Hsu, "U.S. to Expand Immigration Checks to all Local Jails," *The Washington Post*, sec. Politics, 19 May 2009, http://www.washingtonpost.com/wp-dyn/content/article/2009/05/18/AR2009051803172.html (accessed 04 October 2010).

[55] Bolle and others, *Guide to Biometrics*, 31.

[56] Ibid., 35.

individualized identifiers.[57] The ability to credibly identify individuals by the use of fingerprints proved immediately useful in the realm of criminology and has been used heavily in related fields as well as the public sector ever since.

Perhaps the most notable development in fingerprint analysis, which is pertinent to immigration and border control, was the incorporation of computer processing that occurred in the 1960s.[58] Since then, numerous manufacturers have continually developed and improved the technologies and equipment used in the collection, processing, and subsequent comparison of fingerprints. The culmination of advances in automation and processing capability allowed for fingerprints to become the main identification source for state agencies such as the U.S. Federal Bureau of Investigation (FBI)[59], as well as prominent international organizations such as the International Criminal Police Organization (INTERPOL.)[60] The systems and technology that are used to acquire, process, and search fingerprint databases is commonly known as automated fingerprint identification systems (AFIS) and are continually incorporated into identification and screening systems today. The ability to use AFIS and rapidly share information through computerized technology reinforces the role of fingerprints in verifiable identity through the creation of digitally searchable and instantly sharable information.

In biometrics, the traditional methods of collecting ink fingerprints have largely given way to "livescan" techniques, which actively scan fingerprints through the use of an electronic device. These captured systems are typically based upon one or a combination of the following methods and technologies: (1) reflection technologies,

---

[57] Ronald K. Noble, "Opening Remarks: 5th INTERPOL International Symposium on Fingerprints" (Lyon, France, INTERPOL, 4 June 2008), http://www.interpol.int/public/ICPO/speeches/2008/SGFingerprints20080604.asp# (accessed 01 October 2010).

[58] Keith A. Rhodes and U.S. General Accounting Office, *Information Security Challenges in using Biometrics* (Washington, D.C: GAO-03-1137T, September 2003), 7, http://www.gao.gov/new.items/d031137t.pdf (accessed 17 February 2010).

[59] By the 1950s it is estimated that the FBI database contained over 110 million fingerprints and developed AFIS by 1960. Watner and McElroy, *National Identification Systems: Essays in Opposition*, 97.

[60] INTERPOL adopted a standardized AFIS in 1996. Noble, *Opening Remarks: 5th INTERPOL International Symposium on Fingerprints*.

which use light to capture minutiae details; (2) capacitance methods, which rely on electrical charges to map individual minutiae; (3) thermal sensing, which creates a minutiae map using variance in temperatures; or (4) ultrasound, which uses a beam of sound to map or measure the differences between different minutiae.[61] While these methods of capturing and analyzing fingerprints are continuously refined, the quality of the capture can often determine the usefulness of the print. The physical and environmental conditions prevalent on an individual finger such as moisture, cleanliness, or finger pressure on the capture device can also cause significant differences between captures, although these issues are being rapidly corrected through improvements to collection systems. Despite these issues, fingerprints are currently the most proliferated and recognized biometric identifiers that when paired with advanced computer technologies have the potential to provide widespread and reliable access to verifiable identification and authentication.

### *c. Iris Scan*

Iris scanning is one of the more recent biometric identifiers that may be more promising than facial photos and fingerprints in achieving verifiable identity. The main advantage of iris scans over other biometric identifiers is their notable increases in accuracy when used for authentication.[62] Although iris scans are not as widely accepted by the public as facial photos and fingerprints, literature is beginning to reflect that as an individual human identifier "iris scanning appears to be the most robust and most accurate" biometric identifier currently available.[63] Using the iris as a biometric identifier is a fairly simple process that involves capturing an image of the iris and subsequently computing the prominent features with algorithms designed for pattern recognition.[64] The ability to process an iris scan is independent of eye color, and the eye

---

[61] Bolle and others, *Guide to Biometrics*, 33.

[62] John G. Daugman, "High Confidence Visual Recognition of Persons by a Test of Statistical Independence," *IEEE Transactions on Pattern Analysis and Machine Intelligence* 15, no. 11 (1993), 1148.

[63] Garfinkel, *Database Nation: The Death of Privacy in the 21st Century*, 57.

[64] Li and others, *Advances in Biometric Person Authentication: 5th Chinese Conference on Biometric Recognition, SINOBIOMETRICS 2004, Guangzhou, China, December 13–14, 2004, Proceedings*, 539.

has some natural properties that protect against falsification of this specific biometric.[65] Border control and immigration programs today are largely focused on facial photos and fingerprints, but there are already existing provisions within many border control identification systems to accommodate the use of iris scans.

Some of the strengths of the human iris as a biometric identifier are: (1) the physical characteristics of an iris are not genetically determined; (2) the iris pattern is developed before birth and does not vary substantially over time (as can facial photos and fingerprints); (3) the error probabilities associated with iris scans are much more favorable than those of facial photos or fingerprints; (4) iris scanning technology is less vulnerable to falsification or forgery; and (5) the processing time for comparing iris scans is exceptionally fast, which makes it ideal for use in screening applications.[66] Despite these advantages, there is a fair amount of public stigma about the intrusiveness of capturing iris images.[67] This perception is likely due to the fact that the acquisition process can be perceived as more intrusive than a simple electronic palm reader or a quick digital photograph. Despite these difficulties, it seems that the superior performance of iris scanning in human identification will result in the further investigation and use of this highly desirable identifier for use in identification and authentication.

### 2. Using Biometric Identifiers

Biometric identification can be useful in the traditional roles of establishing identity and authenticating known identities, but their use in immigration can extend well beyond these traditional roles. Through the use of computer technology, biometric identifiers are being increasingly used to quickly and accurately screen individuals

---

[65] Jain, Bolle and Pankanti, *Biometrics: Personal Identification in Networked Society*, 118–119.

[66] Ibid., 104–120.

[67] When deciding on the biometric identifiers to be included in ICAO mandated Machine Readable Travel Documents (MRTDs), several biometric identifiers were compared for usability, compatibility, redundancy, perception, storage capability, and performance. Based on the expected performance in these areas, facial photographs were chosen as the primary biometric identifier with fingerprints and iris scans being included as secondary identifiers. Mary K. McMunn, "Machine Readable Travel Documents with Biometric Enhancement: The ICAO Standard," *ICAO MRTD Report* 1, no. 1 (2006), 25, http://www2.icao.int/en/MRTD/Pages/ICAOMRTDReport.aspx (accessed 24 May 2010).

against a known set of identities, identify previously unknown individuals, and assign verifiable identity to new individuals in a more reliable manner than traditional nomenclature based methods. Understanding the practical methods by which biometrics are put into use is essential to develop an understanding of how specific biometric identifiers and systems should operate.

Practitioners and decision makers also need to be somewhat familiar with the reliability issues associated with individual biometric identifiers and the systems involved in their capture and processing. This section will further describe some of the specific templates of the biometric identifiers discussed above and explain some of the theory and systems used for various biometric matching and screening systems. A brief introduction to error rates is also included to explain the dialogue often encountered when pursuing identity solutions using biometric identifiers. Understanding how biometric identifiers are used, as well as the literary conventions used when discussing biometric performance, is crucial to understanding biometric systems and their utility in border control.

#### *a. Templates of Identifiers*

The ability to capture, store, process, and share biometric identifiers is highly dependent on the standardization and integration of computerized equipment. Facial photographs, fingerprints, and iris scans as they are currently used in biometric identification are all processed as a certain type of digital image. These images can be further broken down and described as *pixels* or the smallest distinguishable unit within an image. The color characteristics of the individual pixels within the image can then be translated into bytes capable of being analyzed, stored, or exchanged using computers.

There are a number of different capture devices currently available to capture and record biometric identifiers, all with varying levels of detail or different technological capabilities. For these devices to properly exchange information in a useable format for the processing systems, the information needs to be standardized. The formats and standards for biometric information are regularly addressed by different standards agencies, both national and international in an effort to promote the usability of

identifiers and compatibility between systems.[68] The ultimate goal is to provide the ability for select biometric identification equipment to be capable of capturing and relaying data in a format that can be commonly shared, accessed, and processed for use in solving the identity problem.

Facial photographs are perhaps the easiest identifier to capture and record digitally, the recommended standardized format is essentially a digital picture formatted to either conventional RGB standards or the newer electronic JPEG formats.[69] The photographs stored upon (or perhaps within) identification cards are typically intended to be used for identification and authentication largely by human inspectors conducting a visual inspection, however, many systems are beginning to offer the ability to conduct fully automated electronic comparisons as well. The electronic comparisons are typically conducted between stored images contained in a database or within a token (e–Passport) and an actual live capture photograph, matching images would indicate identity authentication. This is part of the intent of shifting to biometric enabled travel documents as highlighted by the ICAO standards.[70] As such, photographs used for identification remain largely the same standard color passport photograph that most are used to seeing on international documents.

Fingerprint data is somewhat more complex but still relies on an imaging device that can capture and characterize the minute details of the skin. Whether fingerprints are taken via ink or "livescan", the standardized format for fingerprint data is a digital capture processed as either a binary or a grayscale image. Inked fingerprints are often scanned into an image while "livescan" prints are converted directly by the capture system. Fingerprint images of individual fingers are relatively small in size and often several images are stored together to represent a full set of prints. The difference

---

[68] The current International Standard for biometric data is published as a joint venture between the ISO (International Organization for Standardization) and the IEC (International Electrotechnical Commission) and is a series of publications under the heading ISO/IEC 19794.

[69] R. Michael McCabe and Elaine M. Newton, eds., *American National Standard for Information Systems - Data Format for the Interchange of Fingerprint, Facial, and Other Biometric Information - Part 1,* (Gaithersburg, MD: American National Standards Institute, Inc., May 2007), 140, http://www.nist.gov/itl/ansi/upload/Approved-Std-20070427-2.pdf (accessed 2 October 2010).

[70] International Civil Aviation Organization, *Machine Readable Travel Documents: Specifications for Electronically Enabled Passports with Biometric Identification Capability*, II–11.

between binary and grayscale formats is that binary describes individual pixels as either black or white (1 or 0) while the grayscale format assigns a pixel one of 256 different shades of grey.[71] The American National Standards Institute (ANSI) also prescribes a corresponding resolution of either high or low for each method, which equates to either 250 or 500 pixels per inch.[72] This essentially equates to four different image formats that can be exchanged between systems and subsequently processed with proprietary software. Minutiae details for each print can are also processed in association with the fingerprint and similarly converted into a digital image format that can be shared electronically. In addition to these conventional formats, there are also a few proprietary systems and formats for fingerprints that can be safely exchanged through electronic media using similar labeling methods but retaining high levels of confidentiality between users.

Iris scans are also typically captured, recorded, and shared as digital images in a very similar fashion as facial photographs. In many cases, the same equipment is used to process an iris scan as is used to capture a normal digital photograph. Some of the newer iris scan devices are designed to incorporate security measures such as pupil measurements to check for liveness and glare assessments to check for contact lenses or glasses worn by an individual. The actual processing of the iris image occurs in the same manner as in the facial photograph with either an RGB color scheme or using the grayscale method to standardize the data. Both methods are acceptable as they accurately convey the distinct markings contained within the human iris with enough fidelity to allow processing and analysis. The iris images tend to be somewhat smaller in size than either facial photographs or fingerprints when stored in the conventional manner and seem to have characteristics that allow for much faster indexing when used for comparisons.[73]

---

[71] McCabe and Newton, *American National Standard for Information Systems–Data Format for the Interchange of Fingerprint, Facial, and Other Biometric Information - Part 1*, 6.

[72] Ibid., 17.

[73] In theory, iris codes can be compared at up to "160 Million codes per second." Daugman, *High Confidence Visual Recognition of Persons by a Test of Statistical Independence*, 1159.

The following table summarizes the ANSI recommended standards for the sizes of select biometric identifiers by dots (or pixels) per inch and lists the allocated space that set aside within the e-Passport Machine Readable Travel Documents (e-MRTDs) for storing biometric identifiers digitally within the document.[74]

**Approximate Size Conversion of Digital Biometric Identifiers**

As Prescribed by ANSI-NIST–ITL 1–2007

| Identifier | Typical Individual Image Size | Average # of Pixels | e-Passport Capacities |
|---|---|---|---|
| Facial Photograph | 1in x 1in (300dpi) | 90,000 | 15-20 kB |
| Fingerprint | .7in x .5in (500dpi) | 87,500 | 100 kB* |
| Iris Scan | .5in x .5in (512dpi) | 65,536 | 60 kB* |

*Currently the e-Passport format allows 10kB per finger image and 30kB per iris image for storage (which add to 100kB and 60kB total storage capacity.)

Table 2. Size Conversion of Digital Biometric Identifiers

These digitized biometric identifiers can also be securely converted through the use of cryptology, ensuring the privacy and protection of individual biometric information.[75] The ability to package biometric identifiers in a digital form allows for the secure transmission prevalent between electronic communication equipment. Most of these identifiers can be passed between agencies in under a second—even with their accompanying header information. Part of the reason that biometric identification is becoming a viable solution in border control and other identity applications is the advances in computer technology that has allowed agencies to digitize biometric identifiers. Translating human identification characteristics into a manageable image format allows an individual's unique and distinguishable traits to be quickly captured, transported, stored, or retrieved.

---

[74] International Civil Aviation Organization, *Machine Readable Travel Documents: Specifications for Electronically Enabled Passports with Biometric Identification Capability*, II–8.

[75] Sachar Paulus, Norbert Pohlmann and Helmut Reimer, eds., *ISSE 2006–Securing Electronic Busines Processes* (Wiesbaden, Germany: Vieweg (GWV), 2006), 197, http://www.springerlink.com/content/g075k556151058n1/fulltext.pdf (accessed 26 May 2010).

### *b. Comparisons and Matching*

Identifiers may be used in a myriad of ways in solving the identity problem from verifying that a presented fingerprint is the same a another stored copy to attempting to determine the identity of an individual solely from an identifier. These processes of comparing and matching biometrics each have unique attributes and individualized solutions when used for authentication and/or screening. This section will describe some of the common authentication and screening operations that are performed my matching or comparing biometric identifiers with respect to immigration and border control. Using biometrics to solve identity problems often depends upon the extent of comparison that needs to be accomplished in order to determine whether or not a match exists. Matching known individuals to their biometric identifiers is relatively simple, while screening to detect matches from a large database can be quite complex.

One method of matching is the comparison of known entities using biometric identifiers. Authenticating a known individual against a known biometric template is perhaps the most basic task that can be performed, often with amazing precision and speed. Matching an individual to their preestablished biometric template is fairly simple and often called a *one–to–one* match. The process can be accomplished in a myriad of ways, but typically requires an existing recorded biometric stored on a token or within a database and a "livescan" biometric from which to compare features.[76] In this case, the biometric system only has to determine if the "livescan" sample matches the existing template. This type of match is often quick since the only computation is the comparison algorithm between the biometrics. In immigration and border control one–to–one matching is used in biometric systems to confirm whether or not a supplied facial photograph or fingerprint matches the recorded template stored on a biometrically enabled passport or within a system database.

Another matching problem that can be solved using biometric identifiers is to attempt to match a known sample to another identifier in larger sample. This type of match is commonly referred to as a *one–to–many* type of match. This type of match can

[76] Bolle and others, *Guide to Biometrics*, 24.

be used for identification or authentication depending on the specific application. In immigration or border control applications this type of operation is commonly used in screening functions.[77] Immigration applicants provide biometric identifiers that are then compared with a database in order to determine if they are a match to any of the known individuals contained within the sample, such as a terrorist watchlist. Processing this type of matching function can take more time and typically depends on the number of samples that require comparison, or the size of the database. The individual characteristics of fingerprints and iris scans lend naturally to classifications that allow them to be catalogued by similarity. This increases the speed of matching operations by only allowing computations on samples that are a likely match. As of 1998, it was reported that "only fingerprint and eye technologies are proven to have acceptable recognition rates to be practical for one–to–many matching."[78] Since then, there have been several technological developments in facial recognition, which are beginning to yield similar recognition rates.[79]

### *c. Recognition and Error Rates*

Measuring the accuracies of biometric systems when it comes to matching individual identifiers is often discussed in terms of recognition rates. The methods and convention for labeling these recognition rates can differ slightly depending on the system design or potentially the commercial manufacturer. Regardless of the nomenclature used, these rates are based the probability of a biometric system being able to match a pair of identifiers that are a true match or reject a pair of identifiers that do not match. The possible errors that can occur based on this expected outcome are: (1) matching a pair of identifiers that are not a true match; or (2) not matching a pair of identifiers that are a true match. For this discussion these errors will be labeled as False

---

[77] Bolle and others, *Guide to Biometrics*, 26.

[78] A. Jain, "Fingerprints: Proving Ground for Pattern Recognition" (Hong Kong, 2006), http://www.comp.hkbu.edu.hk/~icpr06/final-program.pdf (accessed 10 Nov, 2009).

[79] See "3D Face Recognition Using Stereoscopic Vision" and "A Face Recognition System Based on Local Feature Characterization" in Massimo Tistarelli, Josef Bigün and Enrico Grosso, eds., *Advanced Studies in Biometrics: Summer School on Biometrics, Alghero Italy, June 2003, Revised Selected Lectures and Papers* (Berlin, Germany: Springer, 2005), 135, 151.

Accept or False Reject for identification and False Negative or False Positive for screening, which is in line with some of the more current discussions on biometric error rates.[80] In immigration and border control, the occurrence of these errors can range from a slight inconvenience to a state unknowingly allowing a terrorist to enter its borders.

Depending on the purpose of the biometric identification system, authentication can be of a positive or negative nature and errors can cause substantially different implications. Positive authentication is when a person provides a fingerprint that is a match to the fingerprint stored on file or within a passport, essentially verifying an individual. Negative authentication is when a person provides a fingerprint and it is cross-checked against a watchlist database and found not to match any of the known terrorist templates, otherwise known as screening. Many would tend to agree that in this scenario, errors in the negative authentication portion could be potentially more devastating. The following table illustrates some of these different errors, how they are commonly termed, and how they could potentially manifest in an immigration or border control situation.

**Types of Biometric Identification Errors in Immigration and Border Control**

| Type of Error | Authentication Type | Identity Problem | Result |
|---|---|---|---|
| False Accept | Positive | Verification | Grants Entry to Unauthorized Person |
| False Reject | Positive | Verification | Denies Entry to Authorized Person |
| False Negative | Negative | Screening | Fails to Flag Known Terrorist |
| False Positive | Negative | Screening | Flags Person Who is Not a Known Terrorist |

Table 3. Types of Errors in Immigration and Border Control

Understanding the types of errors that are possible in a matching scenario is essential in assessing individual biometric matching technology and biometric matching systems as a whole. Many of the current systems marketed are advertised along with their expected or proven error rates. Properly assessing the accuracy of a specific biometric matching system must involve the measure of both error rates, as well

[80] Bolle and others, *Guide to Biometrics*, 69,80.

as some knowledge as to how they were obtained.[81] Taking these issues into account, the following table is a generalized approximation of the current error rates of biometric matching systems that a user can reasonably expect to obtain (realizing that this largely depends on the type of biometric equipment and the intended use.)[82]

**Commonly Published Error Rates of Biometric Matching Systems**

| Identifier | False Reject | False Accept |
|---|---|---|
| Facial Photo | 10-20 % | .001-.01 % |
| Fingerprint | 3-7 % | .001-.01 % |
| Iris Scan | 2-10 % | ≥0.001 % |

Adapted from an article by Bolle, Ratha and Pankanti titled "Performance Evaluation in 1:1 Biometric Engines," and published in *Advances in Biometric Person Authentication*, Springer, 2004.

Table 4. Error Rates of Biometric Matching Systems

In this representation of error rates, it is clear that the False Accept rates are much lower than the False Reject rates for every identifier. This may lead to very accurate identification verification systems, but in screening applications a much higher False Reject rate would be desired. Based on the implications of these error rates in different matching situations (verification vs. screening), the debate between desired False Accept and False Reject tends to be largely based around the required levels of security that a system needs to provide. Watchlist operations demand a much lower False Reject rate to ensure that potential matches are flagged. Knowing the expected error rates of the matching system and understanding the desired implementation can lead users to make appropriate decisions about which biometric identifier and system to select to best suit the purpose, be it verification or screening.

Depending on the equipment and purpose of the biometric identification task, some systems or matching software can be adjusted to provide more or less accurate

[81] For more techniques on assessing performance and error rates see: James L. Wayman, "Error Rate Equations for the General Biometric System," *Robotics & Automation Magazine, IEEE* 6, no. 1 (1999), 35–48.

[82] Li and others, *Advances in Biometric Person Authentication: 5th Chinese Conference on Biometric Recognition, SINOBIOMETRICS 2004, Guangzhou, China, December 13–14, 2004, Proceedings*, 44.

rates, which are generally a trade–off between convenience and security. Combining the known identification task with the desired accuracy allows operators to specify the acceptable errors for the biometric system. These considerations can often be dictated by setting desired thresholds for matching or purposefully designing very specific system equipment. Verifying an individual's identity or positive authentication should have a very low tolerance for errors, so that the focus is maintained on only allowing entry to authorized persons. Screening on the other hand may want systems to have somewhat higher tolerance for errors in matching, so that any identifier that may be a close or possible match would be identified by the system. Biometric systems are often designed or programmed based on a specific set of constraints intended to suit the identification purpose and most systems can be constructed or adjusted to reflect the desired matching tolerances. Understanding these fundamental performance indicators and the specific intent of the biometric identification system is crucial when putting biometric identifiers into practical application to enhance state security.

### 3. Biometric System Components and Structure

Moving beyond a basic understanding of biometric identifiers and their individual characteristics, users need to also understand the process and structure of biometric identification systems. The ability to leverage biometrics in a comprehensive identification or screening program will depend on users and managers understanding, managing, and protecting individual identification systems. Biometric identification or authentication systems may have unique attributes, but all share mandatory components that merit discussion. Using biometrics for identification and screening is highly reliant on the interoperability between humans and technology and can be subject to vulnerabilities if not used properly. This section will describe the required processes associated with biometric identification programs building upon the discussion of using biometric identifiers to solve the identity problem. Understanding the components and processes of biometric systems will allow follow on discussion of the specific procedures associated with some of the immigration and border control applications.

One of the more important issues in biometric systems is the creation and maintenance of a biometric database. Databases are used in both identification and authentication by working in conjunction with biometric matching engines. Accurate and useable databases are critical to the process of screening individuals. The ability to capture identifiers, manage the digitized identifiers, and perhaps even share information with others are all very specific functions that can determine the effectiveness of a biometric identification program. Databases will be introduced in this section so as to provide a common understanding of their use in identification applications and present some of the challenges that users and managers may confront when using biometric identification and authentication as a security implement.

Despite the advances and refinements that biometric identification may provide in solving the identity solution, there are still the persistent vulnerabilities that plague every identification system. With a thorough knowledge of these vulnerabilities, designers and users can make efforts to eliminate or mitigate their effects. This section will conclude with some of the types of identification fraud that biometric systems will need to confront in order to maintain their promised gains towards verifiable identification.

#### *a. Typical Program Components*

The ability to construct accurate and reliable biometric identification systems capable of increasing the reliability with which agencies solve the identity problem requires a properly constructed system. The processes that occur within a biometric identification program largely describe the system setup and drive the requirements for equipment and resources. Despite the role, identification or screening, each system follows a general process of acquiring identifiers, storing identifiers, and matching identifiers. The way different systems go about these functions may vary substantially but each function is a required part of the overall method of biometric identification. This section will briefly describe these steps and illuminate some methods that are currently used in immigration and border control.

Acquiring biometric identifiers is essential to performing all subsequent steps within a biometric identification system. This process is often termed *enrollment*

and constitutes the collection of biometric identifiers and their immediate association with a certain individual.[83] This process can vary substantially from voluntary to required and overt to covert, but is essential to begin to implement biometric identification. Enrolling an identifier into any biometric program essentially creates the identity in the program and provides a reference point from which to compare future matches. The quality criteria of enrollment identifiers tend to be fairly high and current systems can often indicate whether an identifier meets the minimum criteria for the specific program. In immigration and border control, this step is often when an individual first applies for a passport and provides a facial photograph and set of fingerprints. The capture and storage of these identifiers and their association with a certain identity is essentially the benchmark of an identity within the biometric identification program.

To use the identifiers that are collected through enrollment or presented for verification, biometric identification systems perform what is commonly referred to as *feature extraction*.[84] This process involves the analysis of the digitized identifier in a format and manner that allows for classification and subsequent use for either identification or authentication. Feature extraction can be quite complicated and is often highly dependent upon the proprietary nature of the biometric identification system. This process can be best described as the translation of a digitized identifier into some discrete value or set of values, which can then be numerically compared with other values. In contrast to the storage standardizations presented earlier for the digital images of identifiers, feature extraction instead refers to the specific pattern recognition methodology, selected algorithms, and template systems that are characteristic of individual biometric identification systems. Often entire identification systems are designed around different feature extraction capabilities. Despite the identification goal or specific identifiers used, each biometric identification system must perform some form of feature extraction. The ability to perform this function directly enables and is often tied to the matching function that often provides the end result.

---

[83] Bolle and others, *Guide to Biometrics*, 7.

[84] Jain, Bolle and Pankanti, *Biometrics: Personal Identification in Networked Society*, 23.

The ability to positively identify individuals through biometric identification relies on the ability to match individual biometric identifiers. This portion of a biometric system is termed the *feature* or *biometric matcher* or simply the *matching engine*.[85] The matching engine uses the extracted features of submitted biometrics and compares them against each other mathematically to determine whether or not they can be considered to be the same sample. Based on the matching function that is desired and the acceptable level of accuracy; the identifiers are compared as appropriate. The matching engine is often proprietary, usually contained within the system software, and can be tied to the feature extraction methodology. These matching engines are based on statistical pattern recognition methods and often programmed to the specific applications (customized towards either security or convenience.)

For one–to-one matching engines, one identifier is set as the baseline or reference identifier (typically the one obtained in enrollment) and is then used as the basis for which to compare the submitted identifier. In a one–to–many matching engine, the submitted identifier (typically obtained via livescan) is set to the baseline and then the entire dataset is compared to the livescan capture in an effort to discern if there is a stored identifier that could be considered a match. These matching tasks can be substantially different in the way they are processed and vary with respect to the biometric system, the selected identifiers, and the acceptable or desired error rates. Pattern recognition is the field of study that deals with the nuances of the biometric matching engines. This field of research is currently experiencing unprecedented growth with respect to biometric identification. Efforts continue to be made that enhance the ability for machines to compare biometric identifiers and pattern recognition studies continue to improve the accuracy and usefulness of biometric identification systems.

Understanding the components of a biometric identification system allows for appropriate decisions to be made in regards to the suitability of effectiveness of an individual system. Each biometric identification system will necessarily have component parts that process enrollment, feature extraction, and some sort of matching engine.

[85] Jain, Bolle and Pankanti, *Biometrics: Personal Identification in Networked Society*, 22.

Biometric identification systems can contain multiple components that perform these functions or be combined with other separate systems depending on the desired design and required capabilities. The basic design and implementation of these systems and eventually how they are put into practical application will depend largely on the capabilities of the system components. Combining these functions into a coherent system or assessing an "off the shelf" system will require the investigation to the enrollment, feature extraction, and matching engine functions with respect to accuracy, speed, and cost. Understanding the design and function of the basic biometric identification systems should provide the background and context required to understand many of the programs being put into practice in the security realm.

#### *b. Biometric Database*

An essential part of any biometric program that may not necessarily be a part of the system itself is the construction, maintenance, or merely access of an accompanying database capable of providing biometric identifier information. Databases used in biometric identification can be physically integrated or disjoined from the rest of the biometric identification system. Databases can be customized for the feature extraction or matching engines or merely masses of standardized digital identifier templates. The ability to create, manage, and successfully extract biometric data from a database is an integral function and a topic much debated amongst researchers and practitioners alike.

The requirement for an accompanying database in biometric identification is largely predicated upon what portion of the identity solution is being solved. Applications for basic biometric identity confirmation may be as simple as placing a collected identifier upon a token (ID card) and verifying the user via livescan techniques against the identifier upon the token. In this instance, the "database" is the single identifier stored on the token, in many circumstances a very usable form of identification. Extending beyond this to a screening function such as using terrorist watchlists, could drive a much different requirement—potentially one calling for a precise, secure, and most likely confidential database. Often in practical applications, multiple databases are

accessed for varying portions of the identity solution.[86] Determining the type of database that will be used in biometric identification is an important consideration in system design and implementation.

### *c. Biometric Vulnerabilities*

Biometrics can substantially enhance traditional efforts at discerning verifiable identity, but are still vulnerable to attacks on either the user or the system. Traditional identification routines relied upon an individual having or knowing something like a token or password. Biometrics eliminates the necessity for individuals to keep track of a physical item or retain the exclusive knowledge of a password by incorporating their individual physical characteristics into the identity solution. Biometric identifiers are not subject to being lost or forgotten, but are still subject to forgery attempts or other methods of fraud. The most prominent methods of fraud in biometric identification systems are coercive or impersonation attacks.[87] Many manufacturers of biometric capture devices are countering these impersonation attacks by incorporating software that is capable of determining that an individual identifier is from a live subject and not a facsimile or fake biometric identifier. Databases and digital data must also be protected as they are a large portion of biometric identification systems. The electronic data contained within or associated with biometric identification systems or databases also needs to be protected with respect to availability, integrity, authenticity, confidentiality, and nonrepudiation.[88] Mitigating the known vulnerabilities of biometric identification systems and moving to positively protect the associated information will ensure that incorporating biometric identifiers into identity problem solutions do not allow unnecessary avenues of attack.

---

[86] Using multiple identifiers to contribute to a solution is known as "multimodal" biometrics. An example of fingerprints combined with facial photos is contained in: Lin and Anil, *Integrating Faces and Fingerprints for Personal Identification*, 10 November 2009.

[87] Bolle and others, *Guide to Biometrics*, 214.

[88] Richard C. Schaeffer, *CNSS Instruction no 4009: National Information Assurance (IA) Glossary,* The Committee on National Security Systems, 2010), http://www.cnss.gov/Assets/pdf/cnssi4009.pdf (accessed 01 October 2010).

Biometric systems that are properly constructed and effectively managed have the potential to advance efforts at discerning identity and performing authentication, specifically in regards to immigration and border control. As with any other system, biometric identification is still subject to vulnerabilities that must be addressed and mitigated as these systems are put into practice. Using a comprehensive analysis of the system components, managers and users can work to identify and mitigate many of these vulnerabilities.

Although biometric identification provides avenues to reliably solve the identity problem, it is not immune to attacks or potential problems. Databases and information must be protected and system developers must focus on providing reliable solutions that further reliable identification and authentication. The topics discussed within this chapter should lay the foundation for exploring the merits of specific biometric identification technologies, as well as performing a full system analysis of highly individualized biometric identification systems. Progressing from this point, this work will continue into some specific applications of biometric identification systems as they pertain to immigration and border control tasks and subsequently assess the potential for biometric identification to reduce terrorist incidents within a state's borders.

This chapter has introduced the problem of verifiable identity and explained how the use of biometric identifiers are being put into practical applications that have the potential of more accurately discerning identity and authenticating or screening individuals. It detailed the problems associated with attempting to discern individual human identities and subsequently explained how biometric identifiers can be utilized through comprehensive identification systems to further this aim. Properties of facial photographs, fingerprints, and iris scans were discussed in detail to portray their unique characteristics and outline their applicability for use in identification programs. Building upon the individual biometric identifiers, this chapter highlighted common terms and measures of performance for biometric identification systems. Individual processes within broader biometric identification systems were identified and explained to provide a comprehensive understanding of the requirements and tasks these advanced identification technologies are expected to perform.

# III. BIOMETRIC BORDER CONTROLS

Developing world trends are driving unprecedented levels of international mobility, particularly personal interaction and travel across state borders. While the increased interaction and traffic between states can yield rewards in terms of economic gains, increased transparency, strengthened relationships, and even personal freedom—it can also introduce vulnerabilities to potential malevolence. Along these lines, many states are turning to more complicated and capable identification systems as well as streamlining their information sharing processes in an effort to facilitate the safe and effective flow of international human traffic. Biometrics can help strengthen this process by providing accurate and reliable human identification and authentication. Incorporating the use of biometric identifiers into state identification initiatives enhances the ability to positively identify and screen individuals by unique and verifiable attributes. Similarly, the ability to digitally catalogue and compare biometric identifiers largely supplants the reliance upon nomenclature systems for identifying and screening individuals. Improving the discernment and accessibility of verifiable identity enables states to fully participate in the broadening mobility movement knowing that security threats can be better identified and potentially prevented from entering their borders.

As states experience the increasing mobility through their borders and experiment with biometric identification systems, many are discovering the advantages of verifiable identity in securing their populace and state. Throughout the entire immigration process, the ability to conclusively identify individuals through the use of biometrics can drastically increase the accuracy and reliability of the screening process prior to admitting intending immigrants. Obtaining a validated identity prior to entry becomes the norm, while reliance on a human visual inspection or a computerized nomenclature analysis is becoming a purely secondary method. Through swift and efficient information sharing, cooperative states can now benefit with respect to the screening and identification process. The use of physical disguise or reliance upon an alias will no longer be a viable method to remain anonymous when attempting to penetrate a border.

This chapter will introduce some of the changes that are taking place in immigration flows as states become increasingly globalized to illuminate the magnitude of the identity problem when considering the number of people that are actively crossing state borders on a daily basis. Approaching the problem of international migrations and border control, it will focus separately on identification and screening by examining systems designed to address each separate identity problem. Concerning verifiable identification, it will explain in detail the current international effort to move towards biometrically enabled travel documents through the e–Passport program. It will then turn to state specific screening functions by exploring the screening improvements made by the U.S. with respect to the immigration and border control processes. It will conclude by attempting to discern the perceived U.S. security gains from the perspective of biometric integration by assessing recent visa refusal rates. Overall this chapter seeks to illuminate some of the specific biometric identification programs available to states and illustrate their use through some select examples before moving to a larger integrated analysis of biometric borders in countering terrorism.

## A. THE PROCESS OF CROSSING BORDERS

Recent terrorist attacks, such as 9/11 and the Madrid bombings have spurned many states to place greater emphasis on preventing terrorist attacks within their borders, with an increasing focus upon perpetrators that emanate from abroad. As a result, many states seem to be incorporating biometric identification and screening technologies into their immigration and border control programs. The development of biometric solutions aimed at solving the identity problem (identification and authentication) are being incorporated throughout the immigration process and beginning to play a larger role in the screening of immigrants that has been traditionally based solely on nomenclature. Within the U.S. the entire immigration process has traditionally been highly compartmentalized with different agencies controlling different parts. Since 9/11, this process has undergone substantial revisions and concerted efforts have been made to fully incorporate all available assets and agencies to better secure U.S. borders. The use of biometric identification has strengthened the entire process with respect to verifiable

identity, as well as provided unprecedented opportunities to accurately and fairly screen individuals that would have otherwise gone through our borders undetected.

In immigration and border control, the widely accepted solution to the identity problem was the creation of a passport. Traditionally, passports include an identification piece in the form of an individual's name, along with some additional personal information unique to the individual. Identification and authentication are accomplished using the information and comparing the photo to the individual person. This administrative process for crossing state borders remains largely intact today, yet can now benefit from the inclusion of biometric identifiers. This process to enter or cross a border is mainly a three step process. First, the traveler must acquire a suitable identification token, typically a passport. Second, the traveler must apply and receive permission to enter or cross the border, which is otherwise known as receiving a visa. Finally, the individual must perform the actual border crossing where both the passport and visa are verified. The goal of this section is to describe the magnitude of border transits using examples from of U.S. immigration statistics, explain some of the details of the process of crossing a border, and highlight some of the U.S. changes in border control that have come about as a result of the incorporation of biometric identifiers.

### 1. Immigration Background

State borders have been a symbol of sovereignty and often an insular barrier thought to serve as a buffer against unwanted outside influence. It seems, however, that increasing globalization has leveled many of these once formidable defensive barriers and encourages the fluidity of ideas, people, commerce, and sometimes outside national influence across state borders. This overwhelming trend has the ability to positively affect our personal lives, our interests, and our economies but requires greater exposure to unknown identities. As individuals move through and within state borders, validated identity will become increasingly important in determining which individuals will be granted access rights. The ability to present a verified identity along with the ability to convey personal trust of an individual can further the ability of states to provide for common defense without being subject to undue risk. Although newfound mobility is

providing unprecedented interaction among peoples and nations along with increases in prosperity, it similarly presents challenges with respect to security and calls for better methods for the verification and screening of individuals desiring to transit state borders.

Personal mobility and interaction throughout the international community seems to be on a continually increasing path.[89] Societal globalization is facilitated by more efficient transportation, interconnected markets, political convenience and personal preferences. Individuals today may have the most freedom to participate globally than at any point in history and many indicate that this global interconnectedness will continue on an increasing trend. Obviously, with increasing interdependence and economic interactions comes the requisite transit and mobility of the associated populace. This ability to move and interact globally is greatly facilitated by efficient transit through several physical borders, the most prominent being that of sovereign states. Increasing incidences of border transitions will necessitate more efficient systems for establishing and validating identity in order to convey trust and facilitate travel.

For the U.S., the creation and growth of our country has relied on permissive immigration policies. These intending immigrants and visitors, however, present security challenges felt most at our borders. The U.S. immigration and visa statistics are one testament to the increasing global mobility that nations now experience. In 2008, the U.S. issued non-immigrant visas to just over 6.6 million people, while immigrant visas were issued to slightly less than 500,000 people.[90] While the nearly 7 million people who are annually granted the privilege of entering the U.S. on some sort of official visa program alludes to the immigration numbers, it surprisingly underscores the magnitude of the problem of providing accurate and efficient border controls. The U.S. Department of Commerce records of visitation and tourism to the U.S. gives a better idea of the magnitude of traffic imposed upon the U.S. border and our points of entry (POEs).

---

[89] U.S. Joint Forces Command, *The JOE, Joint Operating Environment, 2008 Challenges and Implications for the Future Joint Force* (Suffolk, VA: United States Joint Forces Command, Center for Joint Futures, 2008), http://www.jfcom.mil/newslink/storyarchive/2008/JOE2008.pdf (accessed 02 February 2010).

[90] U.S. Dept of State, "Worldwide Non–Immigrant Visa Issuances Fiscal Years 2003–2008," U.S. Dept of State, http://www.travel.state.gov/visa/frvi/statistics/statistics_4399.html (accessed 14 December 2009).

Information from 2008 shows that roughly 58 million visitors filed paperwork upon arrival at a U.S. port of entry.[91] Adding the transits of U.S. citizens and accounting for the multiple entries allowed some visitors results in over 500 Million travelers that process through our "primary" border inspections every year, [92] of which nearly 279 Million are foreign nationals.[93]

The intrepid flux of individuals through our nation's border creates vulnerabilities easily exploited by those intending to inflict harm on our nation and its people. Especially in light of staggering immigration statistics and the quest to preserve a sense of national security, the issue of providing adequate screening at our borders remains paramount and continues to be the center of many debates. Although few contest the fact that states have the sovereign "right to obtain all the information it deems necessary from people who seek to enter its territory," many contest the methods by which a nation goes about collecting the information in question.[94] Quite often there are fears of inappropriate use of the information obtained, or the potential for unjust profiling of certain groups of individuals.[95] The state must ensure fair yet adequate screening takes place so as not to place its citizens at risk, while maintaining a fairly open border policy for the benefit of the state.

The addition of biometric identifiers can serve a twofold purpose in this securing state borders; verifiable identity can be used as a means of inclusion allowing citizens to enjoy deserved social benefits, while also securing against outside threats through the process of screening. This ability to further the accuracy of verifiable identity in border control programs makes biometric identifiers a credible tool in mitigating a nation's risk

---

[91] U.S. Dept of Commerce, "Office of Travel & Tourism Industries," U.S. Department of Commerce, http://tinet.ita.doc.gov/view/m-2008-I-001/table1.html (accessed 14 December 2009).

[92] Jennifer E. Lake, *Border Security: The Complexity of the Challenge* (Washington, D.C: Congressional Research Service, Library of Congress, January 2007), 1, http://www.fas.org/sgp/crs/homesec/RL32839.pdf (accessed 11 December 2009).

[93] Randolph C. Hite and U.S. Government Accountability Office, *Information Technology: Homeland Security Needs to Improve Entry Exit System Expenditure Planning* (Washington, DC: GAO-03-563, June 2003), 5, http://www.gao.gov/new.items/d03563.pdf (accessed 19 January 2010).

[94] Baldaccini, *Counter-Terrorism and the EU Strategy for Border Security: Framing Suspects with Biometric Documents and Databases*, 31.

[95] Amoore, *Biometric Borders: Governing Mobilities in the War on Terror*, 336.

to known criminals and terrorists. The advent of established borders, which began as walls and evolved to the complex biometric systems we have today, still serves the same purpose, guarding the social benefits of a certain populace while providing for collective defense. The challenge as state borders become increasingly transited will be adequately securing a populace against those that intend to access borders for the sole purpose of bringing destruction and harm.

### 2. Immigration Process

States use various methods to screen citizens and intending immigrants, which includes both visitors and permanent immigrants. Immigrant screening in the U.S. has experienced some substantial changes mainly due to concern over immigration overstays and the 9/11 terrorist attacks. The events drove several U.S. agencies to acquire systems capable of providing better fidelity for immigration and border control. Many of these systems sought to improve the ability to track U.S. immigrant entrance/exit data, perform reliable identification and screening, and better integrate data with both internal and external agencies. This section will outline the general process of the U.S. immigration screening procedures in order to provide a general backdrop to better understand where biometric systems may prove applicable in immigration and border control programs. The U.S. procedures are perhaps a bit more evolved than many other states, but in general are reflective of the basic process. Despite the state specific system, this section is designed to highlight the utility of biometric identifiers in the different stages of identification, authentication, and screening as it relates to immigration and border control.

#### *a. Passport—Visa—Border*

Immigrants intending to enter the U.S. are subject to a three-step process that involves a series of identification and authentication measures, which eventually yields authorization to enter the U.S. border. The process is largely standardized amongst states and follows the following sequence: (1) the individual obtains a passport within the host nation; (2) the individual then applies for a visa to visit or immigrate to the

destination state; and (3) the individual travels to the state and submits the passport and visa at the border to gain entry. Individuals are identified, authenticated and screened at various portions of the process and in slightly different manners. The passport is ultimately the identification token that can be authenticated by U.S. officials, and the visa is the states permission to enter the U.S. border.[96]

This largely three part system allows states to first evaluate the overall acceptability of the intending immigrant then allows individual states (the U.S. in this case) to determine the eligibility for a visa. If a visa is granted and travel ensues, the individual's identity can again be validated and authenticated prior to gaining entry into the state in question. This process is similar for most nations and largely provides three opportunities to identify a potentially undesirable immigrant, which typically occur at the varying steps of the immigration process. These separate steps in the immigration process present somewhat different challenges concerning identity and authentication, and can build upon each other depending on the system. All three steps must be completed in succession before individuals are granting authorization to enter a state. The process also tends to incorporate different agencies and organizations at each step, although the collective work is aimed at ensuring the acceptability of an intending immigrant.

#### *b. Improving Identification–Authentication–Tracking*

The immigration process is not overly complex, yet it can suffer from intentional nefarious activity or simply inadequate methods to identify or authenticate individuals. Throughout the process states have actively sought to improve their ability to verify and screen individual immigrants in an effort to increase security. Identity authentication and screening often occur at all three points of the immigration process ensuring that an individual is not identified as a threat at any point. Biometric screening programs enhance all three portions of the process by ensuring that both created and

[96] There are some programs that waive the requirements for a visa such as the Visa Waiver Program (VWP) in the US and the generally accepted rules throughout member nations of the EU, but all of the programs ensure that the screening process is thorough and require biometrically enabled documents at the actual border crossing.

authenticated identities are legitimate, that identities are adequately vetted through digitized screening programs, and potentially illuminating attempts of malevolent actors to circumvent or advantage the system. The digital format of these identifiers also enables quick and efficient use of electronic databases throughout the screening process and even at the actual border crossing.

The tangible benefit of biometric integration into the immigration process is the discovery of individuals that have been able to falsify identification records in previous systems. Counterfeiting, forgery, and imposters are the three main types of passport fraud, with the preponderance of abuses being reported as imposter fraud. The U.S. experienced over 13,000 incidents of U.S. passport or border crossing card fraud in 2009 alone.[97] Before the incorporation of biometrics most of the physical passport fraud in the U.S. was committed by an individual using their photograph with another individual's information—a process that is largely preventable through biometric authentication.[98] Biometric identification systems also reduce the chances that nefarious individuals known to governments can effectively use a passport that was created with their actual information as they will most likely be detected through the screening process.[99] The ability to store and share identifiers also allows multiple authentications at a single step. This allows states to compare the individual's identity to the recorded biometric within the travel document as well as with a biometric stored within a remote database. Advances in electronic protection of the individual documents also reduce the chance that an individual travel document can be intentionally manipulated after

[97] Nabajyoti Barkakati and U.S. Government Accountability Office, *Border Security Improvements in the Department of State's Development Process could Increase the Security of Passport Cards and Border Crossing Cards* (Washington, DC: GAO 10-589, 2010), 7, http://www.gao.gov/new.items/d10589.pdf (accessed 16 July 2010).

[98] Jess T. Ford and U.S. Government Accountability Office, *State Department Improvements Needed to Strengthen U.S. Passport Fraud Detection Efforts: Report to the Committee on Homeland Security and Governmental Affairs, US Senate* (Washington, DC: GAO-05-477, May 2005), http://www.gao.gov/new.items/d05477.pdf (accessed 10 August 2010).

[99] This method was used by several al–Qaeda operatives before biometrically enabled documents. Oriana Zill, "Crossing Borders: How Terrorists use Fake Passports, Visas, and Other Identity Documents," *Frontline Reports* (2010), http://www.pbs.org/wgbh/pages/frontline/shows/trail/etc/fake.html (accessed 10 August 2010).

biometric data is assigned.[100] The result is a much more highly integrated immigration system from passport application to the actual border crossing. Increased continuity between agencies and information sharing between states can enhance the security of the immigration process.

## B. BIOMETRICS IN IMMIGRATION

The merits of biometric identification are becoming more evident to many states, as evidenced by the rate at which biometric identification systems are being incorporated into state immigration and border control programs. As of 2008, there were over 61 states that are openly using biometric screening programs.[101] The overwhelming majority of these states were relying upon the ICAO e–Passport biometrically enabled travel documents.[102] The range of identification systems at use within these states spans the spectrum and the inclusion of various proprietary and shared databases is becoming the norm. States are also beginning to realize the benefits from requiring biometric identifiers in travel documents.[103] Many of these successes are only government and news reports of increased denials, deportations, or identified duplicate applicants, but there certainly seems to be some perceived benefit based on the numbers of states that are actively pursuing programs.

This section will discuss some of the specifics of the ICAO e–Passport program as well as the U.S. specific US–VISIT program to illustrate their structures and how they incorporate biometric identification to further increase security in the immigration and border control arena. Focusing on verifiable identification, the e–Passport program is an

---

[100] International Civil Aviation Organization, *Guidlines: Electronic Machine Readable Travel Documents & Passenger Facilitation*, 1st ed. (Quebec, Canada: ICAO Secretary General, 2008), 18, http://www.icao.int/icao/en/atb/meetings/2008/TagMRTD18/TagMrtd18_wp03.pdf (accessed 24 May 2010).

[101] Find Biometrics, *Over 60+ Countries Now Issuing ePassports*, 04 June 2010.

[102] International Civil Aviation Organization, *Guidelines: Electronic Machine Readable Travel Documents & Passenger Facilitation*, 8.

[103] Multiple successes recorded in: U.S. Dept of Homeland Security, "Enhancing Security through Biometric Identification," U.S., http://www.dhs.gov/xlibrary/assets/usvisit/usvisit_edu_biometrics_brochure_english.pdf (accessed 17 February 2010).

international effort to standardize and promulgate the incorporation of biometrics into travel documents in order to assist states in verifying identity. The US–VISIT program builds upon the biometrically enabled documents and represents some of the more robust screening programs that are in use to protect states from nefarious immigrants. Defining the aspects of these programs will allow for a follow–on analysis of biometric identification in relation to terrorist incidents and a comparison of the U.S. immigration rates of refusal for the areas of terrorism and security.

### 1. e-Passport Program—Solving Identification

The International Civil Aviation Organization (ICAO) has taken the lead on addressing the need for verifiable identity within the international community with the advent of the e–Passport program.[104] The term e–Passport is short for electronic passport and is indicative of the overall program aim. The program is largely a set of standards for implementing biometrics into travel documents in order to more accurately and reliable solve the problem of identification. The e–Passport program encourages states to upgrade their traditional passports for a newer biometrically enabled document and has created an international standard for machine readable travel documents (e–MRTDs) ensuring that these documents could be utilized internationally with common equipment. The new passports contain a computerized chip that is able to store biometric identifiers in a common template for use with different state identification programs. The identifiers currently used in conjunction with e–Passport are a mandatory facial photo and the optional inclusion of fingerprints and iris scans.

#### *a. Program Description*

The e–Passport program is the culmination of work that began in 1968 in an effort to better secure passports through the use of computers and speed passengers

[104] International Civil Aviation Organization, *Machine Readable Travel Documents: Specifications for Electronically Enabled Passports with Biometric Identification Capability*.

through the immigration process.[105] In 1998, the concept and study of biometrics was introduced as a form of verifiable identity that could be incorporated into the electronic document.[106] The intent of having a machine readable document with a tamperproof identifier was to cut down on the fraudulent documents and create a readily verifiable tie between the document and the user.[107] ICAO subsequently decided on a format for the document, developed accompanying security protocols, and selected the facial photograph to be the incorporated biometric identifier. The program was finally introduced in 2004 as an international standard for travel documents and is seeing increased implementation by several states as a portion of their immigration and border control programs. The e–Passport document is designed to contain a microprocessor within the document combined with a "contactless mechanism for data transmission."[108] This allows the document to be read simply by being in close proximity to the reader. If used properly, the document provides substantially more information than the previous non-electronic passports. States must decide on protocols and systems to compliment the e–Passport program in determining verifiable identity.

### *b. Identifiers Used*

Incorporating biometric identifiers into travel documents is a largely debated topic with several arguing about the potential privacy issues of digitizing personal information becoming a "slippery slope."[109] Several considerations were taken into account in deciding upon the specific identifiers that would be endorsed for use in a standardized document. The designers weighed the performance of individual identifiers, cost of equipment required to incorporate identifiers, public acceptance and privacy

---

[105] Gildas Avoine, Kassem Kalach and Jean-Jaques Quisquater, "EPassport: Securing International Contacts with Contactless Chips," in *Financial Cryptography and Data Security 12th International Conference, FC 2008*, ed. G. Tsudik (Berlin: Springer-Verlag, 2008), 143.

[106] International Civil Aviation Organization, *Machine Readable Travel Documents: Specifications for Electronically Enabled Passports with Biometric Identification Capability*.

[107] Ibid., II–11.

[108] Eleni Kosta et al., "New Approaches for Security, Privacy and Trust in Complex Environments," in *IFIP International Federation for Information Processing*, eds. Hein Venter et al., Vol. 232 (Boston: Springer, 2007), 467–472.

[109] Ackleson, *Securing through Technology? "Smart Borders" After September 11th*, 67.

concerns, as well as the potential usefulness in state specific applications. After some dispute, the only biometric identifier that will be required to be incorporated into the e–Passport document is a facial photograph, but the documents were also designed with available storage space specifically set aside for fingerprint and iris scan images. The provisions in the document for fingerprints and iris scans are considered optional and left to each state for deciding whether or not to incorporate. The format of the facial photograph contained within the e–MRTD is a portrait size color photograph.[110] The use of the facial photograph was considered to be adequate for enhancing verifiable identification, while still remaining within many of the readily accepted standards for privacy concerning the collection of biometric identifiers.

### *c. Identity Solutions*

Solutions to immigration and border control often rely on a combination of methods to solve identification and authentication, which all have the potential to be strengthened by using the e–Passport program. Depending on the desires and capability of the state, e–MTRDs with integrated biometric identifiers can be used as a standalone program or incorporated into other existing state structures. The incorporation of biometric identifiers into the documents brings a twofold benefit: (1) identities can be validated and screened upon creation of the e–MRTD; and (2) assuming successful creation, the document can be subsequently verified at all other portions of the immigration process. The potential to create a fraudulent document substantially decreases as individuals are required to furnish biometric data at the onset, which is often screened and validated prior to document creation. Similarly, the ability to subsequently alter the document is substantially more difficult than traditional passports. These security measures provide the potential to identify and prevent known malevolent actors from acquiring the means to cross state borders.

Once an e–MRTD is successfully created, the proposed application methods for using the devices outlined by ICAO are commonly known as a *two, three,* or

[110] International Civil Aviation Organization, *Machine Readable Travel Documents: Specifications for Electronically Enabled Passports with Biometric Identification Capability*, II–12.

*four–way check*.[111] The numerical descriptor references the number of independent sources that an e–MRTD biometric identifier is compared against and suggests that the larger the number, the more comprehensive and potentially accurate the verification. The two–way check will be nearly universal to all states but the three–way check will be highly dependent on the state's ability to incorporate a biometric database into the identity solution. The U.S. and EU already have comprehensive databases for this purpose, which integrate well with their specific biometric systems. Although states will most likely employ vastly different identification systems based on their database capabilities, the two–way check will remain a common capability—as will the traditional ability to visually compare the individual presenting the eMRTD with their physical appearance. The following table summarizes these different applications and how they could possibly be implemented in solving the identification problem.

**ICAO Proposed Applications for Biometric Solutions**

| Type of Check | Biometric Matched Between These Sources |
|---|---|
| Two–Way | Livescan–eMRTD |
| Three–Way | Livescan–eMRTD–State Database(s) |
| Four–Way | Livescan–eMRTD–State Database(s)–Visual Inspection |

Adapted from ICAO Document 9303, Machine Readable Passports Volume II, 2008.

Table 5. ICAO Proposed Applications for Biometric Solutions

Despite the selected application and the comprehensiveness of checks that states opt to perform, the development and use of e–MRTDs certainly has the potential to improve the validity and reliability of passports when verifying identity in the immigration and border control process. Creating a permanent biometric tie between the document and the holder that is able to be consistently verified and used for authentication is much improved over the traditional methods of visual verification. The e–MRTD can be used to validate identity at each step and when combined with a storage capability, the process can be used to validate the continuity of identity throughout the

[111] International Civil Aviation Organization, *Machine Readable Travel Documents: Specifications for Electronically Enabled Passports with Biometric Identification Capability*, II–9.

immigration process. The e-MRTD also provides a common template for biometric identifiers that can be used in conjunction with proprietary databases in a variety of screening applications. Overall, the e–Passport program is furthering the case of verifiable identity by incorporating the reliability and permanence of biometrics into common travel documents.

### 2. US–VISIT Program—Improving Screening

Incorporating adequate security into immigration and border control programs relies equally on identity verification, authentication, and authorization. Identity verification provisions have been addressed by international standards, but authentication and authorization are largely left up to individual states. The functions of tracking and screening have always been priorities in immigration and border control, however, the implementation of timely and accurate capabilities has long suffered from the problem of verifiable identity. To better solve these identity issues, states are beginning to refine authentication and authorization processes using biometric identifiers and integrated information sharing.

Concerns about sufficiently screening and accurately tracking immigrants has long been an issue in the U.S. and the events of 9/11 served to intensify the call for better methods to protect our citizens from terrorism stemming from abroad.[112] With immigration processes that were already under scrutiny, the U.S. rapidly implemented biometric based technologies aimed at improving immigrant screening form traditional nomenclature methods to advanced biometric databases that were increasingly integrated and could capitalize on a number of identification characteristics.[113] These advances illustrate the increased screening capabilities that can benefit from biometric

[112] Keith A. Rhodes and Gregory C. Wilshusen, *Information Security: Homeland Security Needs to Immediately Address Significant Weaknesses in Systems Supporting the US-VISIT Program: Report to Congressional Requesters* (Washington, D.C: GAO-07-870, July 2007), 4, http://www.gao.gov/new.items/d07870.pdf (accessed 12 July 2010).

[113] Lisa M. Seghetti and Stephen R. Viña, *U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) Program* (Washington, D.C: Congressional Research Service, Library of Congress, January 2006), http://www.usembassy.it/pdf/other/RL32234.pdf (accessed 09 December 2009).

identification technologies. The following section discusses changes in the U.S. immigration programs in recent years to illustrate the use of biometric identifiers and databases in screening applications.

Administered by the Department of Homeland Security, the United States Visitor and Immigrant Status Indicator Technology (US–VISIT) program was specifically designed to integrate biometrics into the immigration process and provide increased security along our national borders by improving the tracking and screening ability of our immigration systems.[114] US–VISIT sought to capitalize on the newly developed biometric identification technologies in order to improve U.S. border screening mechanisms. Eventually the program will also incorporate a reliable entry/exit tracking capability for all U.S. immigrants.[115] The basic premise of the US–VISIT program is that biometric identifiers, primarily fingerprints and digital photographs, can be used to identify and subsequently screen all individuals attempting to enter the U.S. through comprehensive and inter–related databases, which will gather, store, and share biometric identifiers.

The requirement for this type of program actually began prior to the events of 9/11 and was centered on the call for an entry/exit program for foreign nationals under the 1996 Illegal Immigration Reform and Immigrant Responsibility Act (IIRIRA).[116] This legislation later combined with several federal mandates from the Dept of Justice, the USA PATRIOT Act[117] and HSPD–6[118] all of which eventually led to the mandatory inclusion of biometric information and forcing information sharing between federal

---

[114] The various laws creating and governing US–VISIT can be found in the Federal Register (Volume 73, Number 245) dated 19 December 2008; Page 77473.

[115] U.S. Dept of Homeland Security, *US-VISIT Biometric Identification Services*.

[116] §110 of IIRIRA is located in Division C of the Omnibus Consolidated Appropriations Act of FY1997. United States Congress, *Omnibus Consolidated Appropriations Act, 1997* (Washington, DC: U.S. Congress, 1996).

[117] As per Public Law 107-56, 115 Stat. 271, 353 (26 October 2001).

[118] United States, *Homeland Security Presidential Directive/HSPD–6 Integration and use of Screening Information* (Washington, D.C: White House, Office of the Press Secretary, 16 September 2003), http://www.dhs.gov/xabout/laws/gc_1214594853475.shtm#1.

systems.[119] Implemented in 2002, the US–VISIT system collects biometric identifiers (currently 10 digit fingerprints and a facial photograph) from specific visa applicants and then accesses several different databases to effectively screen intending immigrants.[120] Since the creation of DHS, and the corresponding awareness of intelligence integration through the Terrorist Screening Center (TSC), biometric screening seems to making large strides in identifying and disseminating potential terrorist or security indicators

Proponents of the US–VISIT insist that it serves as another layered defense against terrorist attacks upon our nation by increasing the ability to identify and hold accountable the many visa applicants intending some sort of harm or potentially attempting to enter the U.S. illegally.[121] On the other hand, opponents consistently point out the overwhelming expense of the system itself as well as the general infringement upon civil rights associated with the program.[122] Despite the stance, many authors and citizens have rightfully questioned the amount of money being dedicated to biometric screening and question the systems capability.[123]

### *a. Origins of U.S. Screening*

The task of successfully screening all U.S. immigrants falls largely upon three distinct agencies—the Department of State (DOS), the Department of Homeland Security (DHS), and the Department of Justice (DOJ).[124] The detailed processes associated with immigrant identity verification and screening responsibility falls

---

[119] Rhodes and Wilshusen, *Information Security: Homeland Security Needs to Immediately Address Significant Weaknesses in Systems Supporting the US–VISIT Program: Report to Congressional Requesters*.

[120] Amoore, *Biometric Borders: Governing Mobilities in the War on Terror*, 339.

[121] Baldaccini, *Counter-Terrorism and the EU Strategy for Border Security: Framing Suspects with Biometric Documents and Databases*, 49; Woodward, *Using Biometrics to Achieve Identity Dominance in the Global War on Terrorism*, 3.

[122] L. O'Brien, "DHS Biometric Program in Trouble," *Wired,* 26 February 2007, http://www.wired.com/science/discoveries/news/2007/02/72792 (accessed 22 January 2010).

[123] Ackleson, *Securing through Technology? "Smart Borders" After September 11th*, 70; Amoore, *Biometric Borders: Governing Mobilities in the War on Terror*, 337.

[124] Michael John Garcia and Ruth Ellen Wasem, *Immigration: Terrorist Grounds for Exclusion of Aliens* (Washington, DC: Congressional Information Service and the Library of Congress, May 2005), 2, http://fpc.state.gov/documents/organization/48380.pdf (accessed 12 July 2010).

primarily upon two separate agencies, the Bureau of Consular Affairs (CA), which issues visas (under DOS), and Bureau of Customs and Border Protection (under DHS), which is tasked with inspecting all immigrants at our borders or points of entry.[125] Between these two agencies, immigrants are subjected to identity creation and authentication along with comprehensive background checks to determine suitability of visa issuance and then a subsequent screening at the physical border. Biometric identification is now being integrated throughout the process to ensure accurate identity creation and authentication during both the initial screening process and again to at the border.

Before digitized biometric identifiers were available for use in travel documents or screening systems, these agencies relied upon screening methods that relied on "name checks" typically using locally available information and various watchlists specifically constructed for the purpose of keeping out "undesirables". This data intensive process was typically conducted by a Bureau of Consular Affairs (CA) interviewer at a foreign embassy often with limited resources and time. Often this process required checking several different databases and local sources prior to determining suitability for acceptance and visa issuance.[126] Although watch lists were being used by the as part of the screening process well before computers became commonplace, the data was often compiled without any regular consultation or verification between other applicable agencies.

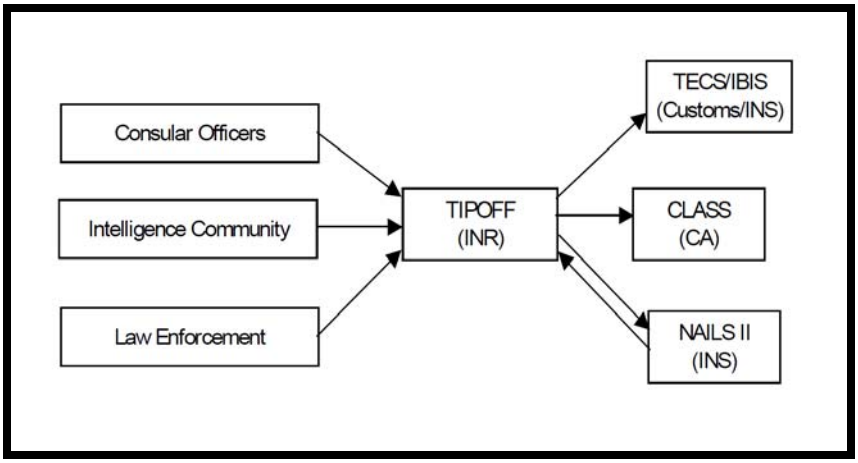
In 1987, the primary database used by the DOS for terrorist screening was known as TIPOFF, it was loosely tied to some other sources of information. Figure 1 below shows some of the structural ties between this early database and the other systems with which it interfaced.[127]

---

[125] William J. Krouse, *Terrorist Identification, Screening, and Tracking Under Homeland Security Presidential Directive 6 (HSPD–6)* (Ft. Belvoir: Defense Technical Information Center, 2004), 5–16, http://handle.dtic.mil/100.2/ADA445120 (accessed 19 January 2010).

[126] John J. Tkacik Jr., "Why the Department of Homeland Security should Control Visas," *The Heritage Foundation* Backgrounder, no. 1569 (2002), http://www.heritage.org/Research/HomelandSecurity/BG1569.cfm#pgfId-998924 (accessed 08 March 2010); Spencer S. Hsu, "U.S. Preparing to Drop Tracking of Foreigners' Departures by Land," *The Washington Post*, sec. 1, 2006, http://www.washingtonpost.com/wp-dyn/content/article/2006/12/15/AR2006121500092.html (accessed 05 March 2010).

[127] The Terrorist Watchlist Connectivity Diagram in Figure 1 was adapted from a 2004 Department of State presentation and printed by Congressional Research Service. See: Krouse, *Terrorist Identification, Screening, and Tracking Under Homeland Security Presidential Directive 6 (HSPD–6).*




Adapted from: Krouse in CRS Report for Congress (RL32366), *Terrorist Identification, Screening and Tracking Under HSPD–6*.

Figure 1. Pre HSPD–6 Terrorist Watchlist Connectivity Diagram.

Although the screening system was not terribly robust, the focus at the time was placed on the efficiency and speed of processing applications. These systems were often developed individually and had accessibility problems preventing meaningful information exchange—primarily due to differing classification levels between the separate systems. Preventing terrorism had not come to the forefront of many of these agencies until the second bombing of the world trade center in 2001, which highlighted several of the interoperability problems between TIPOFF and other related databases. This disastrous attack largely served as the impetus for increasing information sharing and improving U.S. watch list capabilities.[128] As a result, the TIPOFF based screening methods and our ability to track immigrants entering the U.S. came under heavy scrutiny as many of the 9/11 hijackers either slipped through the immigrant screening process despite having terrorist indicators or violated the limits prescribed by their U.S. visas. These events helped solidify the call for using biometric methods to ensure verifiable identity, reliable screening, and entry/exit tracking.

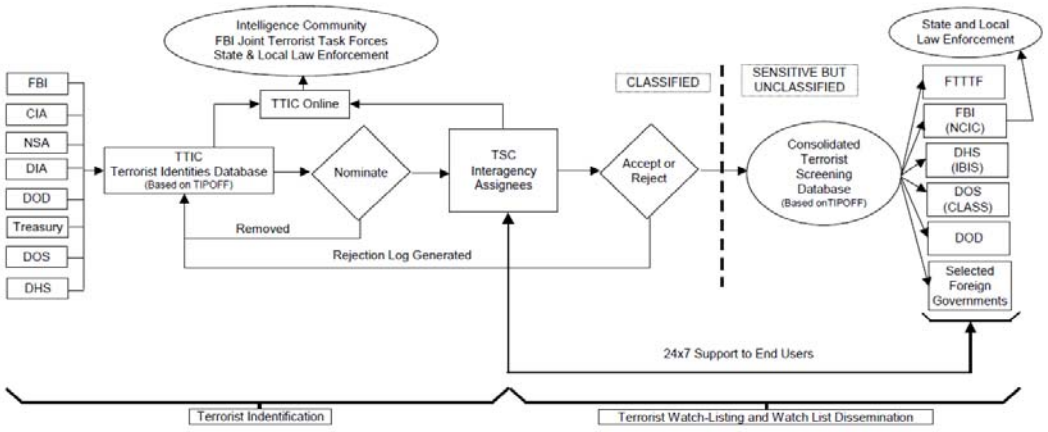
[128] Eldridge, *9/11 and Terrorist Travel Staff Report of the National Commission on Terrorist Attacks upon the United States*.

### *b. U.S. Screening Under HSPD–6*

In an effort to address some of these shortcomings and in turn enhance our ability to detect and prevent terrorist activity, the Bush administration released HSPD–6 in 2003.[129] The guidance contained in HSPD–6 aims to increase the emphasis on terrorist intelligence gathering and information sharing between agencies, improve the U.S. ability to share credible information, pass information between agencies, and facilitate access to appropriate information for the agencies responsible for terrorist screening duties.[130] The most notable contribution of HSPD–6 was the creation of a centralized database containing all available information on known or suspected terrorists known as the Terrorist Screening Database (TSDB), which can be accessed by all applicable U.S. agencies. The agency responsible for maintaining the TSDB and handling all functions pertaining to U.S. watchlist activities is the Terrorist Screening Center (TSC.) Making the TSC central to the screening process encouraged the use of common architecture and facilitates the sharing of information between agencies at all levels of the spectrum—including national, state, local, and tribal jurisdictions. The resulting structure and mandated agency interaction prescribed by HSPD–6 is illustrated in the figure below.

[129] United States, *Homeland Security Presidential Directive/HSPD–6 Integration and use of Screening Information*.

[130] Ibid.




Adapted from: Krouse in CRS Report for Congress (RL32366), *Terrorist Identification, Screening and Tracking Under HSPD–6*.

Figure 2. Terrorist Identification and Watch Listing Under HSPD–6.[131]

As the focal point for U.S. immigration screening activities, the TSC is highly reliant on the ability to gather, share, and fuse intelligence data—then in turn, pass actionable information to distributed agencies, mainly end user screeners. The TSC maintains a 24–hour call center that assists screening agencies when individuals are flagged as being a match to the TSDB and ensure the appropriate agency is able to handle the specific problem. The creation of the TSC can be considered a large success in streamlining screening functions as evidenced by the volume of terrorist watchlist matches that have been documented.[132] In addition to terrorist watchlist matches, other agencies are also reaping the benefit of improved tracking and identification of U.S. immigrants. Overall, the U.S. immigration enforcement agencies are credited with well

[131] Inter-agency flowchart as printed in - Krouse, *Terrorist Identification, Screening, and Tracking Under Homeland Security Presidential Directive 6 (HSPD–6)*.

[132] "Between December 2003 and May 2007, the TSC has documented more than 99,000 encounters for which its call center was contacted, with over 50% of the calls being a positive match to a terrorist watchlist identity." U.S. Department of Justice, *Follow Up Audit of the Terrorist Screening Center* (Washington, DC: Audit Report 07–41, Office of the Inspector General, Audit Division, September 2007), http://www.justice.gov/oig/reports/FBI/a0741/final.pdf (accessed 11 August 2010).

over 500,000 immigration related apprehensions per year.[133] The ability for a state to create, maintain, and quickly access reliable information that can be used in screening functions is becoming a mandate in protecting state borders. Successful screening mechanisms directly support immigration enforcement actions and this integrated structure allows all agencies faced with an identity problem to quickly access the required information to make an appropriate decision. Overall, HSPD–6 has furthered the capability for all U.S. agencies to share critical information and greatly enhanced screening programs that should reduce the likelihood that a known suspect could easily penetrate the U.S. border with the intention to conduct criminal or terrorist activities.

### 3. U.S. Visa and Immigration Refusals

Measuring the effectiveness or quantification of biometric identification in immigration can be difficult, but there are some signs that the U.S. is seeing tangible successes after the inclusion of biometrics through US–VISIT and the improved watchlisiting capabilities under HSPD–6. Exploring the quantitative change in U.S. immigration enforcement actions in the areas of security and terrorism should illustrate how the incorporation of biometric identifiers into the primary U.S. identification and screening mechanisms has influenced the effectiveness of our border security measures. The ability to deny entry to an increasing number of applicants based upon verifiable identification and screening procedures is certainly one desired result of incorporating biometric identification into immigration and border control programs. This measure may not be the most precise or accurate indicator of the contributions of biometric identifiers in the immigration process, but it seems to be a common performance metric presented by states as a way to assign merit to biometric identification and screening. The supported hypothesis is that changes in biometric identification and screening have enabled the U.S. to prosecute and deny increasing numbers of immigrants for security and terrorism concerns.

---

[133] U.S. Department of Homeland Security, *Immigration Enforcement Actions: 2009* (Washington, DC: Office of Immigration Statistics, 2009), http://www.dhs.gov/xlibrary/assets/statistics/publications/enforcement_ar_2009.pdf.

The rigorous U.S. screening process is designed to maintain security by not allowing nefarious individuals to gain access to U.S. borders. The Immigration and Naturalization Act (INA) contains all the laws that govern the U.S. visa refusal categories, of which this study will only consider the number of ineligible immigrants from the *Security and Terrorism* category, as defined by each individual law listed below:[134]

| | |
|---|---|
| 212(a)(3)(A)(i) | Espionage, Sabotage, Technology Transfer |
| 212(a)(3)(A)(ii) | Other Unlawful Activity |
| 212(a)(3)(A)(iii) | Activity to Overthrow the U.S. Government |
| 212(a)(3)(B) | Terrorist Activities |
| 212(a)(3)(C) | Foreign Policy |
| 212(a)(3)(D)(i) | Immigrant Membership in a Totalitarian Party |
| 212(a)(3)(E)(i) | Participation in Nazi Persecutions |
| 212(a)(3)(E)(ii) | Participation in Genocide |

The ability of the U.S. to identify ineligibles as they are subjected to the biometric screening process will be assessed using available open source data, using the U.S. Department of State report on *Annual Visa Ineligibles*.[135] The annual numbers of ineligibles will be compared against the backdrop of biometric developments within the U.S. programs. The two major developments in screening during this time period were the inception of biometric identifier collection through US–VISIT in early 2002, and the subsequent changes to the screening programs that occurred through the implementation of HSPD–6 in late 2003. Each program has evolved since inception, but 2002 will be used as the definitive timeframe where biometric identifiers were compensatory for U.S. immigrants and 2004 will be the first year where the improvements of HSPD–6 could be considered to have been effective. The analysis of annual ineligibles will be assessed both as a whole and keeping in mind the developments in U.S. immigration associated with these dates. The annual numbers of ineligibles will also be normalized over the number of immigrant applications in order to account for quantitative changes in

[134] § 212(a)(3); 8 U.S.C. § 1182(a).

[135] Can be found at http://travel.state.gov/visa/frvi/statistics/statistics_1476.html.

immigration activities. These constraints should allow for an objective and quantifiable analysis of the effectiveness of U.S. immigration and border control agencies at preventing entrance to individuals known to pose a credible threat to U.S. security.

The last section has shown how after HSPD–6, the Bureau of Consular Affairs agent adjudicating visas for foreign applicants now has access to many of the biometric screening databases through their respective database with potentially more accurate and integrated information. Although, U.S. visa refusals have traditionally relied on information from U.S. databases, the advent of biometric screening brings with it the prospect of information sharing with other states and localities. The ability to share data outside the conventional agencies, incorporate foreign government biometrics databases, and access other agencies captured biometrics should provide increased capability to refuse immigration benefits to potential terrorists or known criminals. This is creating a vested interest in sharing data between states as many believe this will yield collective security gains.

The U.S. has always sought to protect its borders against known terrorist threats, but also places an importance on maintaining a fair and unbiased system that supports fair and robust immigration. The grounds for inadmissibility under the INA security and terrorism concern are aimed at individuals who "have engaged or intend to engage in terrorist activity either as an individual or as a member of a terrorist organization."[136] Although the specific reasons that individuals denied entry are not discernable nor are they releasable to the public, the aggregate numbers for each category are regularly published and updated. The following chart contains the collective numbers from the "Immigrant and Nonimmigrant Visa Ineligibilities" section of the *Report of the Visa Office* available from the U.S. Dept of State website.[137]

---

[136] Ruth Ellen Wasem, *Immigration Visa Issuances and Grounds for Exclusion Policy and Trends* (Washington, D.C: Congressional Research Service, Library of Congress, March 2010), 13, http://assets.opencrs.com/rpts/R41104_20100310.pdf (accessed 27 March 2010).

[137] U.S. Dept of State, "Visa Statistics: Report of the Visa Office," http://www.travel.state.gov/visa/statistics/statistics_1476.html (accessed 14 October 2010).

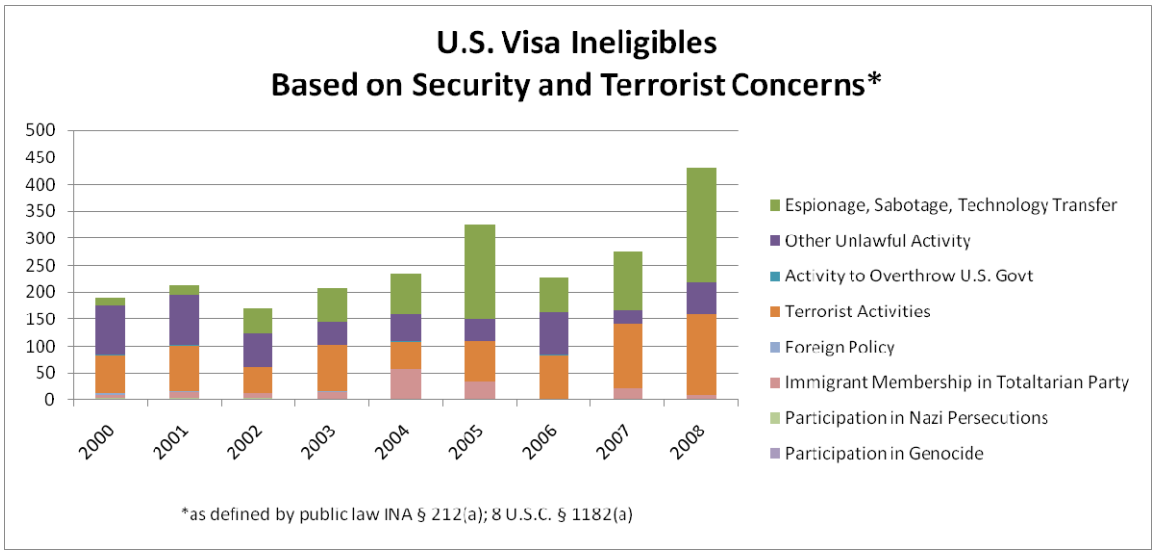



Figure 3. U.S. Visa Ineligibles for Security and Terrorist Concerns.

Analyzing the data for U.S. ineligibles, it is apparent that there is an increasing trend in the cumulative numbers of individuals denied entry at our borders across the entire period. There are also some categorical changes between different individual INA categories. Since biometric screening became fully integrated in 2004, there appears to be marked increases in the area of *Espionage, Sabotage, Technology Transfer* and the area of *Terrorist Activities*. Arguably these areas could receive the greatest benefit from biometric screening and database integration. One notable issue that can now be addressed through these technologies is an applicant who attempts to gain a U.S. visa through multiple applications, often with different names. With the incorporation of biometric information on each visa application, name is no longer the primary identification method and now these offenders can be readily identified through biometrics and subsequently denied entry, depending on the circumstances.[138]

[138] Biometric Example - "A female Peruvian, married to a British National, applied for a UK settlement visa in Spain. She said that she had not applied for a UK visa before, however a biometric check revealed a match to a male applicant for a visa in Madrid earlier in the year. When interviewed she said the male applicant was her brother but was unable to explain the fingerprint match. Further examination of travel documents revealed that she had made a previous application, which had been refused, using her brother's passport but replacing his photograph with hers. The second application was also refused." M2 Presswire, *Ten Point Plan for Border Protection and Immigration Reform; First Milestone Met as Fingerprint Checks Go Global.*, 1.

Perhaps the most pronounced change is between 2002 and 2005, where US–VISIT began collecting and processing biometric identifiers from all U.S. immigrants. These four years show increases in cumulative numbers denied entry as well as distinct increases in the category *Espionage, Sabotage and Technology Transfer*. Looking closer at this category, there were 14 individuals denied entry in 2000—which increased to 213 individuals by 2008. This area shows both cumulative and progressive increases in denials since the incorporation of biometric identifiers through US–VISIT, as well as the improved information sharing under HSPD–6. The second most notable characteristic is the increases in terrorist based refusals that began in 2006 and extended through 2008. Refusals based on the terrorism concern had remained fairly steady from 2000–2004, but then exhibit large increases in the years 2004–2008. This would be an expected result of a vastly improved and comprehensive watchlist system that began operating in 2003. These two increases would be indicative of the expected benefits from achieving better identification solutions and being able to more accurately prosecute screening activities.

Positively attributing these increases to either US–VISIT or the TSC would require much more specific information, but as a collective result, it certainly appears that there are noticeable increases in terrorist based refusals that are evident immediately after these programs commenced operation. These increases in refusals in these two areas while all others remain relatively steady certainly indicate that there may be some connection between biometric identification and improved screening and the U.S. ability to refuse entry to immigrants that may be capable of posing a security risk.

In addition to analyzing the cumulative increases in refusals, there can also be some interpretation of the general trends that may useful in discerning the reasons behind these increases in visa refusals. Taking the same refusal data and plotting a trend line based on the moving average depicted below, shows a steady trend of increasing refusals immediately after the implementation of biometric screening and database integration.

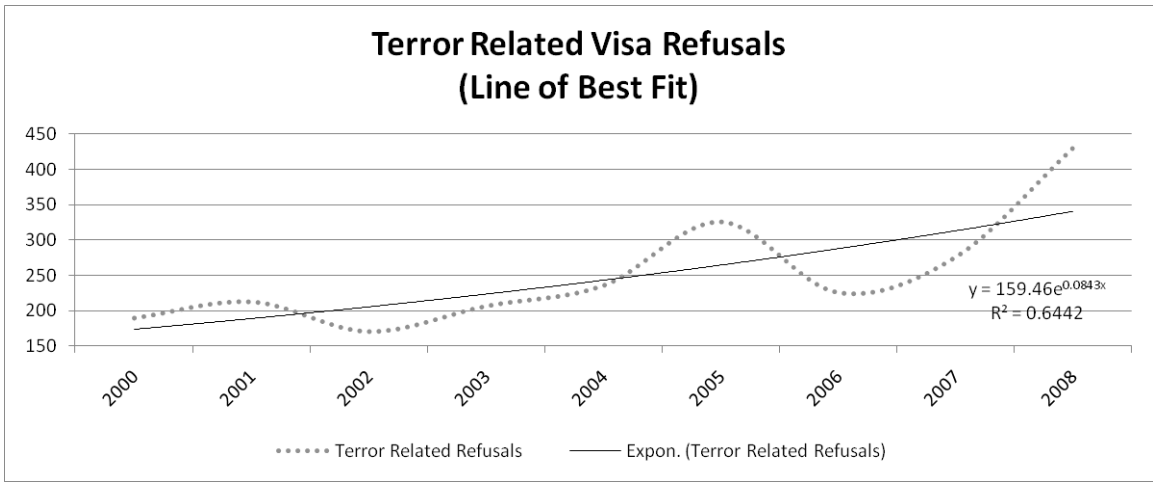



Figure 4. Terrorism and Security Refusal Trend Line.

By using the moving average, trends over time are better reflected around the endpoints. This allows us to analyze the available data immediately around the 9/11 terrorist attacks and more accurately draw out the trends after the implementation of biometric screening in 2002 and improved screening mechanisms in 2004. One interesting observation is that immediately after the devastating events of 9/11, the rate of refusals remained relatively steady. After such a traumatic attack on our nation, one might intuitively assume that U.S. immigration would have been more restrictive in the area of terrorism and security. This data is perhaps the best response to any counterarguments that could claim refusals in these areas could be attributed to an increased vigilance or perhaps based on prejudiced refusal practices.

Some could argue that these increases could be due to a variety of factors and further information is needed to positively ascertain the role of biometric identification in each specific case. Obviously the release of this information could compromise some of the inherent strengths of the identification and screening systems, hence qualitative assessments may not be able to be made based on the public data. This limitation may reduce the ability to positively correlate biometric identification or improved screening to the discernable increases in refusals, but does not invalidate the presence of these increases.

Another interpretation of the visa refusal data, which may reinforce the increased capability to process terrorist information as it pertains to visa issuance, can be represented by the percentage of refusals processed with respect to the number of immigration applications. Normalizing the data in this fashion discounts the fact that the increases noted above could be merely achieved by an overall increase in the number of intending immigrants. Figure 5 reflects the total number of INA refusals under security and terrorism as a percentage and is plotted against the total annual immigration numbers.

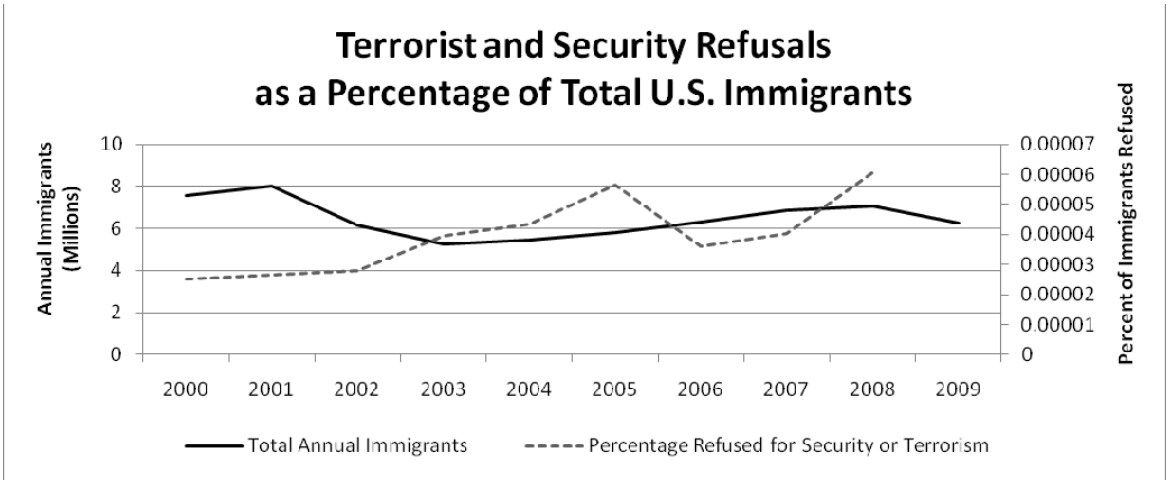



Figure 5. INA Security and Terrorism Refusal Percentages.

Normalizing the number of refusals for the total numbers of immigrants shows that increases in INA refusals are not attributable to increases in immigration. This chart shows that the total numbers of immigrants has actually decreased slightly over the period in question while the actual numbers of refusals has experienced some sharp increases. Translating these observations into immigration and border security terms, the data show that a larger percentage of intending immigrants are being denied entry for security or terrorism concerns. These increases also correspond in time to the beginning of US–VISIT, as well as the changes to our screening systems under HSPD–6. This hints at an increasing ability to flag immigrants as unsuitable, most likely due to the increasing availability of positively identifiable information within the U.S. immigration screening systems.

The fact that the U.S. is able to deny entry to a greater number of immigrants on the basis of validated security and terrorism concerns is one indication that our border security measures may be becoming more effective as a result of biometric identification and improved U.S. screening mechanisms. It is important to keep in mind that these efforts are only one small part of a comprehensive set of programs designed to prevent terrorists from transiting state borders. Biometric identification in immigration and border control is a front line defense aimed at preventing entry to nefarious individuals. Once an individual is within the U.S. border, information fusion is allowing successful infiltration of these nefarious groups by U.S. agents.[139] In border control, or internal counterterrorism efforts, it is becoming evident that the most effective way to prevent plots is through the collaborative sharing of multi-agency information. States must be able to use information in the immigration and border control process to prevent individuals from entering a state and rely upon other agencies to properly use information for identifying and preventing attacks that may originate from within the state. Biometric screening, along with many of our counterterrorism tools, plays a pivotal role in identifying individuals and preventing their access to states that they intend to harm.

This chapter illustrates how the biometric identification processes contained with the US–VISIT program and HSPD–6 guidelines has positively affected the U.S. immigration and border security system. Capitalizing on the use of biometric identifiers in the immigration process has allowed the U.S. to mandate verifiable identity throughout the immigration process and create a robust screening process prior to and at the U.S. border. This system has merited several individual successes as well as contributed to more effective screening at U.S. borders when taking into account the number of effective refusals based on security concerns. HSPD–6 further incorporated all U.S. agencies into the counter terrorism realm by mandating the TSC as well as an improved process for collective information sharing. The ability to share this important data with other U.S. agencies allows for a more comprehensive counterterrorism system. The

[139] Germain Difo, *Ordinary Measures, Extraordinary Results: An Assessment of Foiled Plots since 9/11* (Washington DC: American Security Project, 2010), http://www.americansecurityproject.org/content/wp-content/uploads/2010/05/Foiled-Plots.pdf (accessed 01 June 2010).

ability to harness the reliability of verifiable identification in the immigration process and move beyond the nomenclature based screening systems has the potential to enhance security throughout the U.S. immigration system. Following this standard for biometric identification, combined with a comprehensive and robust database for screening purposes, several other states are now developing proprietary systems for conducting extensive identity screening along their borders in hopes of providing increased security and protection for their citizens.

THIS PAGE INTENTIONALLY LEFT BLANK

# IV. ASSESSING BIOMETRIC BORDERS

Increasing numbers of states are turning to biometrics to enhance border and immigration screening programs. As such, it certainly seems evident that biometric screening will become an integral part of a comprehensive counterterrorism strategy. Proponents argue that the incorporation of biometric identifiers into the screening process helps states to validate individual identities and reduce the ability for individuals to falsify travel and identification documents. Despite the appeal of this claim, no formal studies been conducted that attempt to correlate biometric screening with terrorist incidents. This chapter will attempt to provide a foundation for analyzing the relationship between biometric screening at state borders and terrorist incidents conducted by foreign nationals. Using the first 20 states that implemented biometric screening programs as the target of interest, this chapter will provide a quantitative analysis of biometric screening initiatives and terrorist incidents form 1991–2007. The goal is to begin to develop metrics that might be used to assess the contributions of biometric screening programs to the reduction of terrorist activities across state borders in order to justify the merit of such systems. Effectively protecting borders with biometric technology will rely on the development and implementation of quantitative analytical techniques capable of assessing biometric screening initiatives—a topic with very little publication besides media reports or industry advocacy.

This chapter will focus on investigating the relationship between biometric screening and terrorist incidents in the following ways: (1) comparing the aggregate numbers of (and changes in) terrorist incidents in each state with respect to pre–defined biometric periods based on the implementation of biometric borders; (2) conducting a graphical analysis of terrorist incidents in each state; and (3) performing a statistical correlation of terrorist incidents in each state with the existence of a biometric screening program. Ultimately, this study should provide a foundation for building analytical methods that can be used to measure the effectiveness of biometric borders, their role in state security and their utility in the fight against international terrorism.

## A. BIOMETRIC SCREENING

Biometric screening initiatives are continually growing in number, expanding in scope and consistently adding new capabilities. Currently, there are over 60 states that have incorporated biometric screening into their border protection plans, many using the commonly established machine readable travel documents as defined in the e-Passport program.[140] The first state to establish a national biometric screening program was Malaysia in 1998 with several others that followed suit in 2004–2006, many of which were spurned by the deadline to participate in the U.S. Visa Waiver Programme.[141]

In order to effectively analyze biometric screening in relation to terrorist incidents, it is necessary to be mindful of the recency of these programs. In order to keep this analysis meaningful with respect to the infancy of many biometric programs, it specifically focuses on states that established a biometric screening program on or before 2006. While these programs can be considered to be relatively young, this should allow adequate time since program implementation to detect perceptible changes in terrorist incidents. Since several of the states in this study implemented programs at different times, much of the analysis will be with respect to defined "biometric" time periods based on the states program implementation date. Bounding the analysis in this manner is based upon the following facts: (1) the procurement of biometric systems and building the corresponding databases often takes place over a number of years;[142] (2) depending on the visa replacement programs, many states have differing amounts of time where individuals can still travel with nonbiometric documents; and (3) the terrorist incident dataset does not contain events beyond 2007, which limits analysis beyond this point. As such, this study will focus on the first 20 states to implement biometric

[140] Find Biometrics, *Over 60+ Countries Now Issuing ePassports*, 04 June 2010.

[141] International Civil Aviation Organization, *Guidelines: Electronic Machine Readable Travel Documents & Passenger Facilitation*, 8.

[142] Implementation varies with state procedures and is highly dependent on equipment procurement as well as the time required to bring all state issued visas into compliance. The US initiated limited biometric screening in 2002, but subsequently maximized screening effectiveness with the creation of the TSC in 2004.

screening, with program implementation dates between 1998 and 2006. Table 6 contains the entire list of states in considered in this study sorted by their biometric program implementation date.

| State | Biometric Border Date |
|---|---|
| Malaysia | 3/1/1998 |
| Dominican Republic | 5/1/2004 |
| Pakistan | 10/25/2004 |
| Belgium | 11/24/2004 |
| Thailand | 5/26/2005 |
| Monaco | 7/18/2005 |
| Norway | 10/3/2005 |
| Sweden | 10/3/2005 |
| Australia | 10/24/2005 |
| Germany | 11/1/2005 |
| New Zealand | 11/4/2005 |
| UK | 3/6/2006 |
| Japan | 3/20/2006 |
| France | 4/12/2006 |
| Singapore | 4/29/2006 |
| Iceland | 5/23/2006 |
| Austria | 6/16/2006 |
| Portugal | 7/31/2006 |
| Denmark | 8/1/2006 |
| USA | 8/14/2006 |

Table 6. Date Biometric Screening Established.

The primary data source for terrorist incidents will be the Global Terrorist Database (GTD) for the years 1991–2007.[143] This database contains detailed reports of all recorded incidents that meet the definitions outlined by the National Consortium for the Study of Terrorism and Responses to Terrorism (START). For an event to be included into the GTD database, it must meet certain attributes and criteria. First the event must have at least one of the following attributes: (1) the incident must be intentional; (2) the incident must entail some level of violence or threat of violence; or (3)

[143] The GTD is a product of: START – A Center of Excellence of the U.S. Department of Homeland Security, *Global Terrorism Database*.

the perpetrators of the incidents must be sub-national actors.[144] Additionally, incidents must also meet at least two of the following three criteria: (1) the act must be aimed at attaining a political, economic, religious, or social goal; (2) there must be evidence of an intention to coerce, intimidate or convey some other message to a larger audience than the immediate victim; and (3) the perpetrators of the incidents must be sub-national actors.[145]

Using the GTD dataset, information from specific events within the states of interest will be: (1) standardized by formulation into identifiable terrorist plots for continuity of analysis (explained further below); (2) analyzed with respect to time periods—including before, during and after biometric screening implementation; (3) graphically assessed; and (4) statistically correlated with biometric screening. The first three analytical methods should reveal any existing trends in terrorist incidents in relation to the establishment of biometric screening programs, while the final portion will help determine strength of any perceptible relationship. The hypothesis is that biometric screening prior to and at state borders should lead to noticeable decreases in terrorist incidents—even though biometric screening is only a portion of the entire effort that states are beginning to use to counter terrorism.

### 1. Defining Biometric Screening Periods

To effectively compare biometric screening initiatives in place throughout the world, it is necessary to identify the date of implementation for each states biometric screening program and then define standardized time periods that will be used uniformly for the assessment of individual biometric screening initiatives.[146] Defining and applying biometric screening periods allows for accurate cross-comparison of each state and

---

[144] National Consortium for the Study of Terrorism and Responses to Terrorism, *Global Terrorism Database Codebook 3.0* (College Park, MD: University of Maryland, 2009), 4, http://www.start.umd.edu/gtd/downloads/Codebook.pdf (accessed 01 December 2009).

[145] Ibid., 5.

[146] Biometric screening program implementation dates were taken from various sources, mostly government published documents and media releases from each individual state. Once checked for accuracy, the implementation dates used in this analysis were the same as in: Find Biometrics, *Over 60+ Countries Now Issuing ePassports*, 04 June 2010.

ensures that the analysis of events with respect to implementation is standardized across the different programs. Ultimately the events in the GTD will be separated by the state where the incident occurred and assessed with respect to three separate time periods calculated based on the biometric screening implementation date.

These time periods can be defined as: (1) a prebiometric screening period before program implementation; (2) a transition period defined as the implementation date and extending for 2 full years; and (3) a post-biometric screening period defined as the end of the transition period to present. The prebiometric screening period can be best defined as the timeframe where states were using nomenclature or nondigitized identity verification forms, a practice that entails using nonmachine readable visas without incorporated biometric identifiers. The transition period is defined as beginning in the year that a state reports the implementation of a biometric based screening program at their national borders and continues for a period of two years. Defining this transition period is an important consideration in evaluating biometric screening effectiveness due to the assumption that there is a quantifiable amount of time between the launch of a biometric screening program and the moment in time when equipment and procedures will be fully in place and operating at an acceptable level of efficiency. Most states begin issuing the new biometric visas on the program implementation date but simultaneously create stipulations for travelers to use their existing "nonbiometric" travel documents for a specified amount of time. News articles and literature seem to indicate that most states are accomplishing the complete transition of travel documents over a course of about five years. The two years designated in this study as a "transition period" is somewhat less than the required time that it would take a government to replace every previously issued non-biometric visa, but ample time to allow for screening equipment to be fully functional at state borders. Designating this transition period allows further fidelity to focus on the events that take place during the changeover between nonbiometric and biometric screening programs. The period of time after the transition period is designated as the biometric screening period and represents the end of the transition period to the present, during which it is assumed that previously implemented biometric screening programs have continued to operate without interruption.

These defined "biometric time periods" will be used as the chronological basis for the quantitative assessment of terrorist incidents within each country. Using these time periods will allow for the comparative study of states that may have different program implementation dates. If the addition of biometric identifiers improves the screening process by providing better watch list capability and a platform for validating identity and genuine documents at the border, then there should be an apparent decrease in terrorist incidents after the inception of biometric screening programs. These decreases may be evident in the transition period, but seem most likely to occur in the post-biometric period when screening processes are fully operational.

### 2. Creating Standardized Database Information

In order to effectively assess the role of biometric borders in these countries using the GTD dataset, it is necessary to first standardize and clarify the raw data in order to properly identify and isolate the population of interest in a precise and consistent manner. Events contained in the dataset were analyzed with respect to the identifying information and put into a context that would best allow a high-fidelity analysis. The GTD dataset is largely based on the attack or event specifics but contains relatively little personally identifiable information associated with each event. From this perspective, it made sense to consolidate some of the separate events that were clearly identifiable as a single plot as well as eliminate events that could be readily identified as originating from within a states own borders. It also became clear that in several cases, identifying the known perpetrator would prove elusive resulting in the creation of two separate datasets. One dataset is focused on known perpetrators who have crossed an international border to perpetrate an attack and the other is a group of unknown perpetrators whose origin could not be determined using the information contained within the dataset. The following details the numbers of events contained in the database and describes the modifications that were made to the dataset and the decisions for ultimately using two separate datasets in this assessment.

For the context of this study, the decision was made to consolidate events within the dataset in to readily identifiable terrorist plots, a practice not necessarily used within

the GTD dataset.[147] This decision was based on: (1) the nature of the event data within the dataset; (2) the generally accepted public context of terrorist incidents as being categorized and discussed in terms of recognized plots rather than by separate individuals; and (3) the inability to determine individual perpetrators from many events within the dataset. This also enables a reasonable method to measure aggregate terrorist incidents in a commonly accepted and understandable terminology. For example, the 9/11 attack against the U.S. is coded in the GTD dataset as four events based on the airplanes striking four targets. Rather than translating these events into twenty separate incidents based on perpetrators or remaining as four separate incidents based on targets, it will be treated as a single incident aligned with a single plot. All events in the dataset were adjusted in this manner, as applicable, using mainly the following three pieces of information: (1) the date and nature of the attack; (2) perpetrator information; and (3) attack location. If there was not enough information to categorize similar attacks into a plot, events were left as reported in the original dataset. While this inherently reduces the total numbers, it makes logical sense when comparing aggregate terrorist incidents and should allow for a more commonly accepted terminology when expressed in counter terrorism terms. Another important administrative note is that the GTD data for 1993 was extrapolated in order to addresses the unavailability of data for this specific year (for reasons explained in the GTD codebook.)[148] The following table lists the total number of events for the states of interest that were identified within the dataset at the outset of this research.

[147] National Counterterrorism Center, *2009 Report on Terrorism* (Washington, DC: National Counterterrorism Center, 2010), 3, http://www.nctc.gov/witsbanner/docs/2009_report_on_terrorism.pdf (accessed 07 August 2010).

[148] The GTD dataset does not contain any data for 1993 due to errors in processing and handling information between moves from one location to another—this is explained in the GTD codebook. For this study, incident data for 1993 was fabricated using an extrapolation from the year before (1992), and the year after (1994) and should not significantly affect the results or analysis.

**Raw Database Events by State of Interest**

Data from: GTD (1991-2007)

| State | Raw Events |
|---|---|
| Australia | 43 |
| Austria | 36 |
| Belgium | 40 |
| Denmark | 13 |
| D. Republic | 41 |
| France | 285 |
| Germany | 550 |
| Iceland | 0 |
| Japan | 123 |
| Malaysia | 8 |
| Monaco | 0 |
| New Zealand | 10 |
| Norway | 9 |
| Pakistan | 2198 |
| Portugal | 6 |
| Singapore | 3 |
| Sweden | 31 |
| Thailand | 798 |
| UK | 241 |
| USA | 382 |
| Total Events of Interest | 4817 |

Table 7. Raw Database Events by State of Interest.

Although using the GTD dataset limits this study in currency to the bound of the 2007 information, there are few alternatives to remedy this until the database is updated and expanded to include follow on data. There has been a limited update to the GTD dataset, which includes data through 2008, but at the present time, this data is missing many of the necessary categorical identifiers that would allow the 2008 events to be vetted in a similar fashion as the 1991–2007 data. Alternatively, other databases are available that contain similar information such as the National Counterterrorism Centers Worldwide Incidents Tracking System (WITS), but the criteria for including events into this specific database is constantly changing and does not allow for the similar vetting of individual incidents. As such, even the WITS manual discourages users from attempting

to make annual comparisons using the WITS data.[149] The constraints imposed by using only GTD data are accepted here in order to attain the best fidelity and continuity of information.

### 3. Identifying the Population of Interest

It is also necessary to focus the dataset on the appropriate population, which will allow an analysis of international terrorist incidents in relation to biometric screening along national borders. The population of this study is purposely intended to be those terrorist incidents where an individual or individuals have intentionally crossed an international border in order to take part in an attack. It assumes that the perpetrator crosses the border through a legal method at a time that is proximal to the terrorist incident and that the perpetrator attempted to cross the border with the use of a visa and passport for travel (either genuine or falsified.) While this study does not assess or include illegal immigration, it recognizes that it is a certainly viable and a potential counter to biometric screening initiatives.

Isolating terrorist incidents with an implied border crossing from the GTD dataset is somewhat difficult due to the often incomplete information provided with each incident. For the purpose of this study, the determination to include specific incidents was made by identifying the location of the terrorist incident, the reported perpetrator, and then determining if the perpetrator would have been subject to screening prior to committing the attack. If the perpetrator is not found to be indigenous to the area where the incident occurred, then it is assumed that the perpetrator would have been subject to the process of obtaining a visa, travel documents, and subsequently crossing a state border to accomplish the attack. The screening process (biometric or otherwise) is assumed to take place through these activities, both at the time of visa application and at the actual border crossing. The primary focus of this study will be terrorist incidents where the perpetrator can be reasonably assumed to have originated outside the state border.

[149] National Counterterrorism Center, *2009 Report on Terrorism*, 5.

To identify the terrorist incidents of interest, perpetrator information associated with each event from the GTD dataset will be primarily evaluated by assessing the group or individual name and in some instances, the target type. The "Country_txt" and "Gname" identifiers will be the two primary items used to determine whether a perpetrator originated within a state and would have been subject to screening prior to committing the attack. Perpetrator Information and other data coding classifications are explained in the GTD data codebook.[150] Groups or individuals known to be located within the state where the attack took place will not be considered to have crossed an international border to commit the attack and would not be considered relevant in assessing the screening process. Conversely, any groups or individuals that are known to be located outside of the state where the attack took place were assumed to have crossed an international border to commit the attack. Where the perpetrator origin is missing or is for some reason unclear, other identifying information associated with the individual incident was used to attempt to determine the origin of the perpetrator.

Although the information used in this process (typically the Attack and Target information) varied for individual incidents, most events were relatively straight forward to discern the nature and origin of the attacker. For example, there were a number of U.S. incidents with limited or incomplete perpetrator information and which were not claimed by any certain group. Upon discovering that the targets associated with these attacks were found to be various abortion clinics, these events were disregarded with relatively high confidence that the perpetrator most likely originated from within the state. Other examples were attacks perpetrated by disgruntled citizens (Oklahoma City bombing by Timothy McVeigh), or home based terrorist organizations (such as the IRA throughout the UK.) These groups would not have been subject to any sort of watch listing or identity screening at any point prior to their attacks and hence screening (biometric or otherwise) would never have had the possibility to intervene before the group or individual was able to perpetrate the terrorist attack. Eliminating the identified terrorist incidents that were performed by indigenous groups within the state specific

[150] National Consortium for the Study of Terrorism and Responses to Terrorism, *Global Terrorism Database Codebook 3.0*, 55.

portions of the GTD dataset eliminates these "homegrown plots."[151] The resulting data is a collection of incidents perpetrated by individuals that would most likely have been subject to a formalized screening process at a national border prior to committing the attack. Purposely identifying this population ensures the analysis is focused on screening mechanisms at state borders. The results of this process yielded the events in the column labeled "No Indigenous" as reported in Table 8.

Despite concerted efforts to eliminate terrorist incidents that were found to originate from within the state, there were still several remaining events within the dataset that were coded by perpetrator information described as either "Unknown" or "Other," with little additional information by which to positively identify perpetrator. With a dataset that contained nearly 2000 incidents of interest, events categorized as perpetrated by an "Unknown/Other" made up anywhere from 50% to 100% of each states total events. Revisiting the details of each event perpetrated by an actor classified as "Unknown/Other" in an effort to further discern the origin of these events proved to be exceedingly difficult and arbitrary at best. For example, nearly 70 attacks were classified as an "Unknown" attack committed by an "Unknown" perpetrator. Looking at the attack details seemed to hint that many of these events were most likely performed by indigenous personnel as several attacks were armed assaults on private citizens, assassinations of local persons, and kidnappings of tourists. The following table shows numbers of attacks perpetrated by the "Unknown/Other" perpetrators as grouped by "attack type" to illustrate the numbers and types of events that remained in this "Unknown/Other Included" dataset.

[151] Most determinations of indigenous groups were made by consulting the exhaustive list of state terrorist actors contained in *Political Terrorism*. Alex Peter Schmid and A. J. Jongman, *Political Terrorism: A New Guide to Actors, Authors, Concepts, Data Bases, Theories, & Literature* (New Brunswick, N.J: Transaction Publishers, 2005).

**Numbers of Events Committed by "Unknown/Other" Perpetrators**

Data from: GTD (1991-2007)

| Attack Type | Number of Events |
|---|---|
| Armed Assault | 363 |
| Assassination | 298 |
| Bombing/Explosion | 702 |
| Facility/Infrastructure Attack | 149 |
| Hijacking | 6 |
| Unarmed Assault | 7 |
| Unknown | 41 |
| Total | 1566 |

Table 8. Attack Type Events Committed by "Unknown/Other" Perpetrators.

Due to the variance of information associated with the remaining events and the difficulty in narrowing down the perpetrator identity and/or origin without losing potentially valuable data, the decision was made to create two datasets that would be used for analysis. One dataset includes the "Unknown/Other" perpetrators and the other was created by eliminating any "Unknown/Other" perpetrators.[152] Specifically, conducting analysis using both of these datasets will ensure that the overwhelming numbers of events perpetrated by an "Unknown/Other" actor are not entirely discounted and that the events perpetrated by known foreign perpetrators are analyzed as an independent subset. Table 9 depicts the resulting numbers of events for each state of interest as well as the resulting databases that will be used for analysis.

[152] In order to identify these two different databases within the analysis, they will be labeled "**Unknown/Other Included**" and the "**Unknown/Other Excluded**."

**Database Modifications and Labels***

Data from: GTD (1991-2007)

| State | Raw Events | Internal Actors Removed & Converted to Plots | % *"Unk/Other"* | "Unk/Other" Removed |
|---|---|---|---|---|
| Australia | 43 | 34 | *79%* | 7 |
| Austria | 36 | 17 | *65%* | 6 |
| Belgium | 40 | 24 | *50%* | 12 |
| Denmark | 13 | 8 | *50%* | 4 |
| D. Republic | 41 | 23 | *100%* | 0 |
| France | 285 | 131 | *74%* | 33 |
| Germany | 550 | 191 | *59%* | 39 |
| Iceland | 0 | 0 | - | 0 |
| Japan | 123 | 59 | *88%* | 7 |
| Malaysia | 8 | 7 | *86%* | 1 |
| Monaco | 0 | 0 | - | 0 |
| New Zealand | 10 | 7 | *71%* | 2 |
| Norway | 9 | 8 | *38%* | 5 |
| Pakistan | 2198 | 825 | *96%* | 13 |
| Portugal | 6 | 6 | *100%* | 0 |
| Singapore | 3 | 2 | *100%* | 0 |
| Sweden | 31 | 19 | *73%* | 3 |
| Thailand | 798 | 313 | *90%* | 5 |
| UK | 241 | 47 | *79%* | 7 |
| USA | 382 | 95 | *80%* | 18 |
| Total | 4817 | **1816** | | **162** |
| ***Data set Labels** | | **Unknown/Other Included** | | **Unknown/Other Excluded** |

Table 9. Dataset Creation and Labeling.

After reviewing the specific amplifying data associated with the "Unknown/Other" attacks, it seemed apparent that a rather large majority of the events most likely originated from within the state borders. Although far from conclusive, the information surrounding these attacks, such as target type, attack type, weapon type, location, and even the implied magnitude of the attack seemed to indicate that a majority of these events were associated with groups or individuals that were indigenous. Based on this, it is the author's opinion that even though the "Unknown/Other Excluded" dataset may eliminate a few potential events that might have truly been international terrorist plots, it seems like a more accurate representation of the known

events that originated externally to the state in question. Despite this assumption, both datasets will be evaluated so as to present the most objective view of terrorist incidents with respect to state biometric screening programs.

## B. AGGREGATE ANALYSIS

Once the datasets were narrowed to the incidents of interest, the first portion of analysis conducted was a basic aggregate analysis of terrorist incidents with respect to the defined biometric screening periods (based on each states individual biometric program inception date.) Individual incidents within each state were analyzed as annual averages in each respective time period and the percent decrease is the computation from the prebiometric to post-biometric screening periods. This allows for the comparison of annual events before and after biometric screening, for identifying changes in trends across time, and for comparing general trends within the different states. Again, this analysis is performed for each dataset, the "Unknown/Other Included" and the "Unknown/Other Excluded" as annotated on the figures below.

### 1. Unknown/Other Included Dataset

The generalized result from the aggregate analysis on both datasets shows that all but six of the first twenty countries to implement biometric borders exhibit decreases in annual terrorist incidents between the years of 1991 and 2007. Table 10 depicts the results from the first aggregate analysis using the "Unknown/Other Included" dataset and reports annual terrorist incidents in the predefined biometric time periods with respect to the implementation of a biometric screening program. This provides an initial look at the general trend in annual terrorist incidents across the different countries when grouped by the defined biometric time periods (before biometric screening, during the transition period and after biometric screening.) The annual averages of terrorist incidents depicted show an evident decreasing trend in terrorist incidents over the three time periods, with nearly every state experiencing a decrease in annual terrorist incidents during the transition period, as well as the post-biometric screening period.

**Terrorist Incidents (Events/Year) "Unknown/Other Included"**

By Biometric Time Periods 1991 – 2007

| State | Pre Biometrics | Transition Period | Post-Biometrics | %Decrease in Incidents |
|---|---|---|---|---|
| Australia | 2.82 | 0.50 | 0.00 | **100.00%** |
| Denmark | 0.60 | 0.50 | 0.00 | **100.00%** |
| Dominican Republic | 2.19 | 0.00 | 0.00 | **100.00%** |
| Japan | 4.63 | 0.00 | 0.00 | **100.00%** |
| New Zealand | 0.57 | 0.00 | 0.00 | **100.00%** |
| Norway | 0.61 | 0.50 | 0.00 | **100.00%** |
| Portugal | 0.50 | 0.00 | 0.00 | **100.00%** |
| Singapore | 0.20 | 0.00 | 0.00 | **100.00%** |
| Sweden | 1.75 | 0.00 | 0.00 | **100.00%** |
| Germany | 15.39 | 2.00 | 1.00 | 93.50% |
| Malaysia | 1.00 | 0.00 | 0.13 | 87.50% |
| USA | 7.00 | 1.00 | 1.00 | 85.71% |
| France | 9.87 | 1.00 | 2.00 | 79.73% |
| Belgium | 2.12 | 0.00 | 0.50 | 76.36% |
| UK | 3.60 | 1.00 | 1.00 | 72.22% |
| Austria | 1.13 | 1.00 | 1.00 | 11.76% |
| Pakistan | 47.58 | 36.00 | 91.00 | **Increase** |
| Thailand | 8.61 | 61.50 | 89.00 | **Increase** |

*1816 Incidents ("Unknown/Other Included" for Perpetrators)

Table 10. Terrorist Incidents per Year (Unknown/Other Included).

This result reflects terrorist incidents separated into annual averages with respect to biometric time periods. In this dataset, Monaco and Iceland experienced no terrorist activity during the entire period of study and hence are not depicted. The depicted results show that an overwhelming number of countries experienced decreases in annual incidents over the biometric time periods and only two countries experienced relative increases in the average incidents per year. Of the states that experienced decreases in annual terrorist incidents, several experienced a relatively large decrease in average annual incidents. Overall, this comparison shows relative decreases in terrorist incidents over the three defined time periods in the majority of the countries even despite the inclusion of events in which the perpetrator may have been an internal group or individual. While it is not yet possible to draw conclusions about biometric screening solely on this initial aggregate analysis—it is important to illustrate the trend of

decreasing terrorist activities in the majority of the states after the implementation of biometric borders. It is also evident from this analysis that Pakistan and Thailand stand out from the others in both their increases in annual incidents, as well as their noticeably large numbers of incidents, especially in the post-biometric period. These results prompted further analysis into the states with rather large increases in events in order to: (1) see if there were any notable characteristics of the incidents particular to these countries; and (2) to explore structural or other differences between the states that experienced decreases over the same time periods.

It is immediately evident that both Pakistan and Thailand have at least one portion of highly disputed and difficult to control border that is shared with a neighbor state that may harbor nefarious actors.[153] It was also apparent from the database events that a majority of events in these two states seemed to have indicators that would implicate that several events stemmed from or passed through these troubled border areas. From this perspective, the porous and difficult to control borders of Pakistan and Thailand seem to hamper their biometric screening efforts.[154] In these two countries, even after eliminating known indigenous events, it still seems that the preponderance of events in the "Unknown/Other Included" dataset contain specifics that indicate the events originated from groups indigenous to these troubled border regions. So much so that if "likely indigenous" events (for lack of a better term) are discounted; then terrorist activity within these two countries nearly ceases to exist. This highlights the importance of assessing the nature of the state borders along which biometric screening is being implemented and indicates that biometric screening may have some severe challenges if screening along border crossings is not adequately implemented, secured, and enforced.

---

[153] Jayshree Bajoria, "The Troubled Afghan-Pakistan Border," *Council on Foreign Relations* Backgrounders (20 March 2009), http://www.cfr.org/publication/14905/troubled_afghanpakistani_border.html (accessed 09 August 2010).

[154] CNN iReport, "Thai - Burma Border, Crossing for Food." http://www.ireport.com/docs/DOC-22600 (accessed 06 June 2010); Rizwan Zeb, "Cross Border Terrorism Issues Plaguing Pakistan-Afghanistan Relations," *China and Eurasia Forum Quaterly* 4, no. 2 (2006), 69, http://www.silkroadstudies.org/new/docs/CEF/Quarterly/May_2006/Zeb.pdf (accessed 29 July 2010).

It also brings up the important issue of ensuring that actors are not able to simply circumvent the screening process by crossing either undetected or illegally into another states territory.

### 2. Unknown/Other Excluded Dataset

In an effort to further refine the analysis of average annual terrorist incidents in relation to biometric time periods and focus only on events perpetrated by known external actors, the aggregate analysis was computed using the "Unknown/Other Excluded" dataset. The results were again sorted into the defined biometric time periods and it initially appears that a greater number of countries achieve an even greater decrease in incidents. Although this dataset eliminates a great number of incidents narrowing down to only 168 events, it is most likely the more accurate depiction of terrorist incidents were perpetrated by groups that originated externally to the state. The calculated annual averages for the "Unknown/Other Excluded" dataset are displayed in the figure below and again grouped by biometric time period. With this dataset, five states had no terrorist incidents throughout the periods—Dominican Republic, Iceland, Monaco, Portugal, and Singapore (hence, they are not depicted.)

**Terrorist Incidents (Events/Year)**

By Biometric Time Periods 1991 – 2007

| State | Pre Biometrics | Transition Period | Post-- Biometrics | %Decrease in Incidents |
|---|---|---|---|---|
| Australia | 0.68 | 0.00 | 0.00 | **100.00%** |
| Austria | 0.47 | 0.00 | 0.00 | **100.00%** |
| Belgium | 1.12 | 0.00 | 0.00 | **100.00%** |
| Denmark | 0.37 | 0.00 | 0.00 | **100.00%** |
| France | 2.63 | 0.00 | 0.00 | **100.00%** |
| Germany | 3.14 | 0.50 | 0.00 | **100.00%** |
| Japan | 0.57 | 0.00 | 0.00 | **100.00%** |
| New Zealand | 0.14 | 0.00 | 0.00 | **100.00%** |
| Norway | 0.36 | 0.50 | 0.00 | **100.00%** |
| Pakistan | 1.08 | 0.00 | 0.00 | **100.00%** |
| Sweden | 0.25 | 0.00 | 0.00 | **100.00%** |
| Thailand | 0.43 | 0.00 | 0.00 | **100.00%** |
| UK | 0.57 | 0.00 | 0.00 | **100.00%** |
| USA | 1.37 | 0.50 | 1.00 | **26.83%** |
| Malaysia | 0.00 | 0.00 | 0.13 | **Increase** |

* 162 Incidents ("Unknown/Other Excluded" for Perpetrators)

Table 11. Terrorist Incidents per Year (Unknown/Other Excluded).

Assessing the annual averages of incidents known to be perpetrated by external actors immediately shows a distinct lack of terrorist incidents in the post-post-- biometric time period for nearly all states. Using the same metric of annual averages with the same constraints and time periods, the refined dataset shows that all countries experienced a decrease in terrorist attacks by known entities with the exception of Malaysia. Again, this dataset shows that the annual averages of terrorist incidents experienced a sharp decline in the post-biometric period for nearly all states in the study. Not only did states experience a decrease, many states have not experienced any terrorist incidents in the post-biometric period. While this again is not conclusive evidence that biometric screening at borders reduces terrorist incidents, it certainly highlights a positive trend and illustrates the fact that annual averages of terrorist incidents are numerically declining.

By focusing on known perpetrators who were highly suspected to have been subjected to screening at a state border, this dataset shows that nearly every state had a significant decrease in activity after institution of biometric borders. Additionally, almost every state exhibits a distinct lack of terrorist incidents in the post-biometric period, with the exception of the U.S. (which still experienced a 25% reduction in annual averages.)

As above, these trends are indicative of a reduction in annual terrorist incidents with respect to biometric screening, but do not necessarily imply correlation between these decreases in terrorist incidents and biometric screening procedures. The one certainty from this focused dataset is that there are evident decreases in average annual terrorist incidents over the time period of 1991–2007 for the majority of the countries in question.

## C. GRAPHICAL ANALYSIS

With the exception of Malaysia, most biometric screening programs were put into place starting in 2004 in an effort to bring travel documents in line with the new requirements for machine readable passports prescribed by the U.S. Visa Waiver Programme. To date, many states continue to implement biometric screening initiatives and existing programs are constantly refined (often with biometric identifiers being added to existing programs.) Grouping countries by year provides for programs to be compared with respect to their implementation date and the resulting data to be presented in graphical form. Analysis of these charts shows several general trends perceptible between 1991 and 2007. To best analyze and depict the data, the countries will be grouped by their biometric start dates, where every state with the exception of Malaysia can be grouped into charts for the years 2004, 2005, and 2006.

### 1. 1998—Malaysia

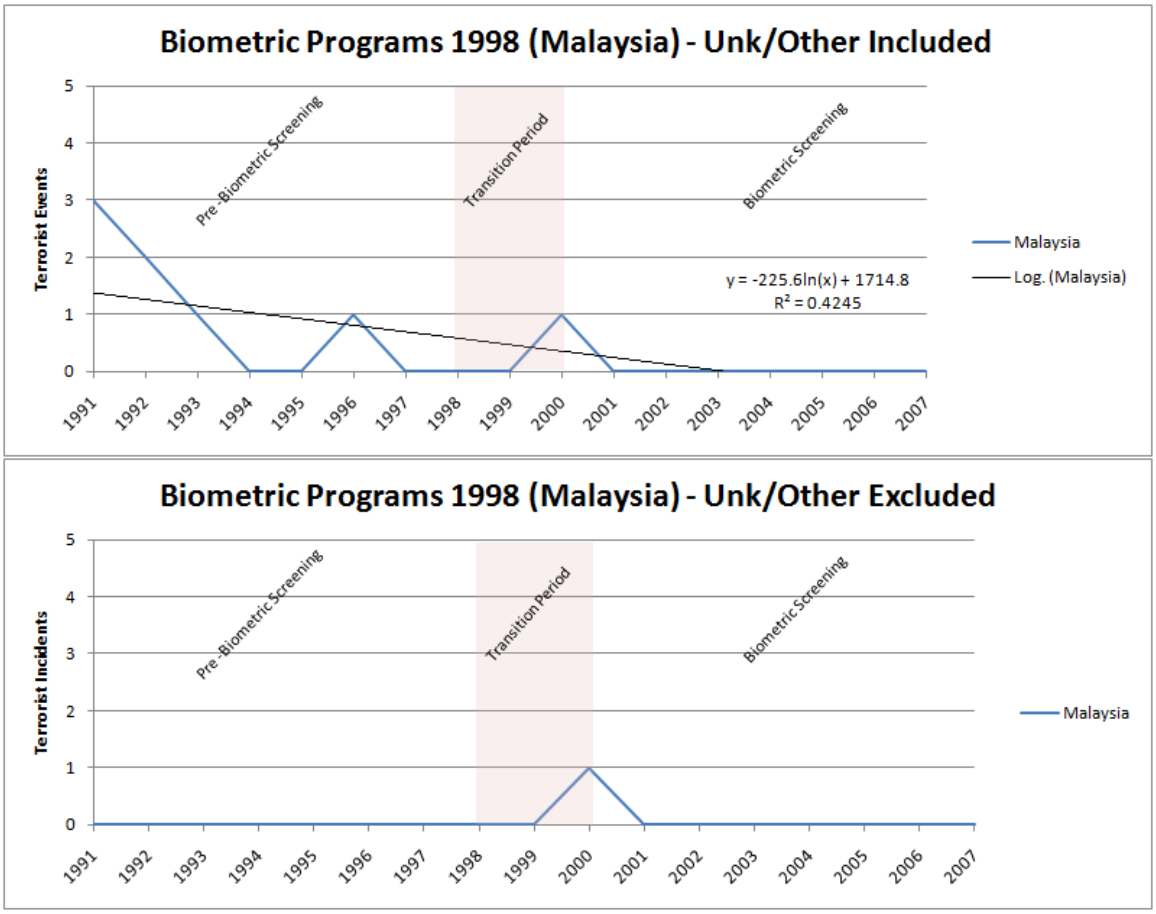



Figure 6. Biometric Screening—1998 Start Date.

Malaysia was the first state to implement a biometric screening program to secure its borders and has very few incidents across the period in question. In both datasets, Malaysia only experienced a single incident after program inception in March 1998. This incident occurred in 2000 during the transition period and Malaysia has subsequently has not experienced any incidents (by known or unknown perpetrators) through 2007. The reported incident in Malaysia was a kidnapping event in 2000 conducted by the Abu Sayyaf Group (ASG) and was the only terrorist incident by a known foreign entity within Malaysia since the inception of biometric screening in 1998.[155] The incident involved a Philippine terrorist group somehow taking hostages from Malaysia, but it is difficult to

[155] GTD dataset event ID# 200004240001 - kidnapping by the Abu Sayyaf Group (ASG), known to operate throughout the Philippines.

ascertain the specific role of border screening with respect to the incident. One notable piece of information was that one of the hostages was later found to be an internal actor of ASG, perhaps indicating that he may have had access to the Malaysian mainland.

Despite the relative lack of terrorist activity, the fact that an attack occurred during the transition period highlights a potential area of concern with biometric screening implementation. Typically, states beginning a biometric screening program based on passport documents do not invalidate existing nonbiometric passports that often remain valid for travel for up to 5 years. This method often allows individuals to continue to travel without being subject to the biometric screening process for various periods, typically between 2–5 years depending on the state. During the transition period, it is expected that several travelers would be able to travel without being subject to biometric screening at the border by using documents issued before biometric screening implementation. This is a good case where further information would be needed to determine if the members of the Abu Sayyaf Group (the alleged perpetrators), which is reportedly based out of southern Philippines were subject to biometric screening at the Malaysian border.[156] Despite this attack during the transition period, the post--transition period is devoid of terrorist incidents indicating that biometric screening may be one of the contributing factors maintaining the relative absence of terrorist incidents in Malaysia.

[156] Larry Niksch, *Abu Sayyaf: Target of Philippine-U.S. Anti-Terrorism Cooperation* (Washington D.C: Congressional Research Service, Library of Congress, 2002), http://www.fas.org/irp/crs/RL31265.pdf (accessed 04 August 2010).

### 2. 2004—Pakistan and Belgium

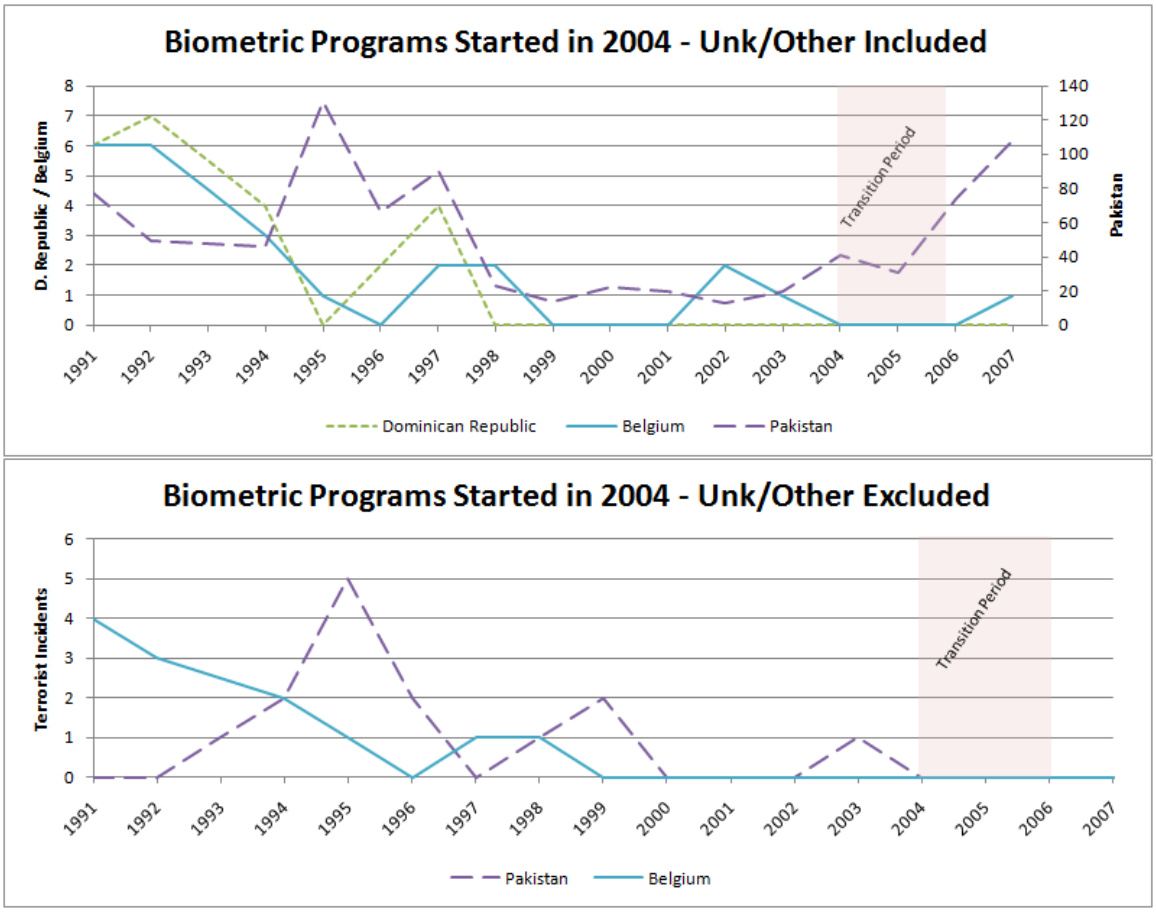



Figure 7. Biometric Screening—2004 Start Date.

After Malaysia, the next group of countries to adopt biometric screening procedures began in 2004, which consisted of Belgium, the Dominican Republic and Pakistan. In the "Unk/Other Excluded" dataset, the Dominican Republic did not experience any incidents that could be classified as perpetrated by a foreign entity and is not included in that corresponding chart. The overall assessment of these states is that both datasets show a mostly decreasing trend. This trend nearly drops to zero terrorist activity for Belgium and the Dominican Republic, but the "Unk/Other Included" dataset shows a sharp increase in attacks within Pakistan after the transition period. These charts also illustrate a general downward trend in terrorist incidents that seems to begin in the mid 1990s.

In the "Unk/Other Included" dataset, Belgium and Pakistan both had terrorist incidents after the transition period; a single event in Belgium and about 180 in Pakistan. Some considerations when discussing the increasing events in Pakistan are: (1) the ongoing war in Afghanistan; (2) the difficulty in implementing border controls along the Durand Line; (3) the overall number of events within this state and region; and (4) the nature of the events within the "Unk/Other Included" dataset. First, the ongoing conflict within Afghanistan and portions of Pakistan against terrorist groups and Muslim extremists undoubtedly affects the overall number of attacks in Pakistan. As mentioned earlier, the region between these two states has traditionally been the origin of numerous terrorist attacks (events in Pakistan alone make up nearly half of the entire dataset in question.) The porous nature of the border between these two states, and the difficulty that the central governments of both states have in controlling the border also create a less than desirable security situation.

It is also important to remember that many of these events are perpetrated by "Unk/Other" perpetrators, whose identities could very well be indigenous. As noted in the aggregate analysis from the dataset review, it seems pretty likely that several of these events are not truly international terrorism and probably originate from the troubled border regions. Looking at the nearly 180 attacks after the transition period, 41 were against military targets, 23 were targeting police, and 67 were directed solely against private citizens. As an example, the following is a summary of one of the deadliest attacks that occurred after the transition period by an "Unk/Other" perpetrator. This specific event occurred in 2007 where several armed assailants (thought to be Islamic extremists) fired upon 85 civilians and 10 soldiers at a mosque in Islamabad, Pakistan; no specific group claimed the attack and hence it was labeled "Unknown" in line with the dataset convention.[157] Since events such as these make up a majority of the refined dataset, they cannot be disregarded entirely but yet don't seem to truly fit the convention of an international terrorist incident. Interestingly, when Pakistan is analyzed with the "Unk/Other Excluded" dataset, the state shows a decreasing trend in terrorist incidents with no events occurring after the inception of biometric screening. Taking this result

[157] GTD dataset event ID# 200707100010.

within the context of the different datasets, it essentially shows that there have not been any "Known" foreign national perpetrators who successfully conducted a terrorist attack within Pakistan since the state established a biometric screening program.

The other anomaly within the "Unk/Other Included" dataset is the attack in Belgium in 2007. This event was a series of Molotov cocktails that were thrown at a number of police stations in the town of Charleroi to which no specific group laid claim.[158] Again, this specific event is a good example of the large number of events that are included in the "Unk/Other Included" dataset but yet are unlikely to be international terrorist incidents. As with the other events in this dataset, there is not enough amplifying information to reject events such as this from the dataset entirely but similarly not enough data to conclusively say that it was an act of international terrorism. Despite this, both datasets show a marked decline in events within Belgium that began before and continued through the implementation of biometric screening programs.

Overall within the states that instituted biometric screening programs in 2004, the incident rates already seemed to be in a steady decline prior to the implementation of screening. It seems that this decreasing trend continued throughout biometric screening program implementation, although there is a slight divergence between the trends in Pakistan within the two datasets. Taking these differences into account, when analyzed from the perspective positively identified or "Known" international terrorist plots, the data show that there have not been any terrorist incidents accredited to a known foreign group during either the transition period or the post-biometric period. This indicates that biometric screening in these states may be one factor influencing decreases in terrorist incidents, at least those conducted by "Known" foreign groups.

[158] GTD dataset event ID# 200702010003.

### 3. 2005—Australia, Germany, New Zealand, Norway, Sweden, Thailand

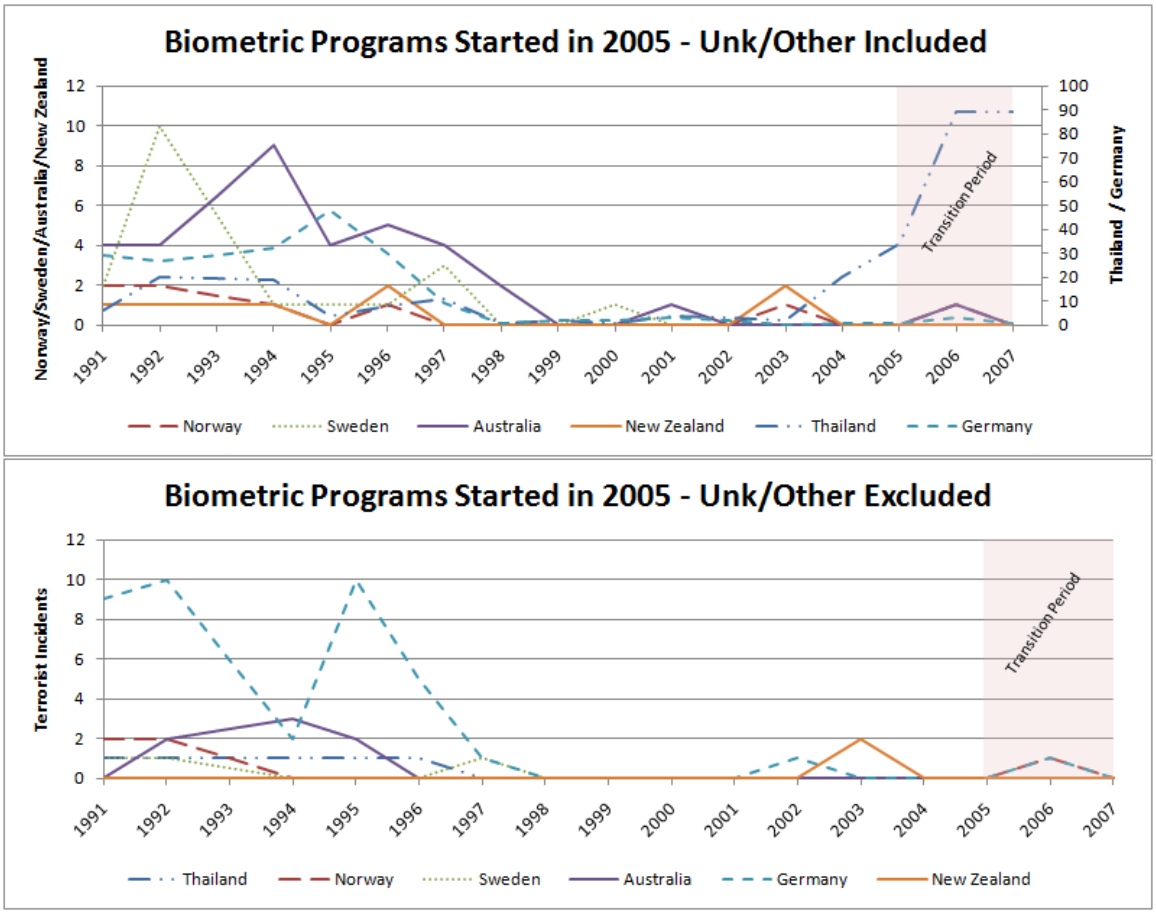



Figure 8. Biometric Screening—2005 Start Date.

In 2005, six more countries added biometric screening programs - many of which were attempting to meet the U.S. deadline for countries to remain in the U.S. Visa Waiver Programme.[159] Similar to the state profiles in 2004, most of these countries had relatively few terrorist incidents per year with the exception of Thailand and Germany (in the "Unk/Other Included" dataset both are on the plotted against the right axis.) Thailand is similar to Pakistan in that they had terrorist incidents that were orders of magnitude greater than most of the other countries in this study and nearly all conducted by "Unk/Other" perpetrators. Germany also had nearly four to five times the terrorist

[159] U.S. Dept of State, "Visa Waiver Program (VWP)," U.S., http://travel.state.gov/visa/temp/without/without_1990.html (accessed 03 June 2010).

incidents per year when compared to the other countries within this group (excluding Thailand "Unk/Other Included" events.) Again, the trend across these states shows what seems to be a wide scale decrease in incidents between the years of 1997 and 2002, and then only a few sporadic attacks, which again decrease to none at the end of the biometric transition period, with the noted exception of the "Unk/Other Included" Thailand dataset.

Looking first at the "Unk/Other Included" dataset, it is evident that: (1) Thailand has a notable increase in incidents slightly before and throughout the transition period and (2) all other states have a decreasing trend in attacks that decreases to zero in 2007. The situation in Thailand is similar to that of Pakistan; the Thai border can be extremely difficult to patrol and has multiple areas that can be breached from neighboring territories with ease. Thailand also suffers from a formidable internal struggle with Muslim extremists that shares carryover with other South Asian countries, as well as political turmoil that may contribute to the large number of incidents in the GTD.[160] Looking through the Thailand specific events committed by "Unk/Other" perpetrators, it again seems apparent that most of the incidents can be directly attributed to these internal conflicts.

Another issue with the biometric screening processes within Thailand is the slow development of the external information sharing and database functions that compliment biometric screening processes. These complimentary programs are now beginning to take shape within this region as the state begins to focus more closely on terrorism. One example of this slow development is the fact that Thailand and Malaysia have only recently agreed to share biometric information on individuals that may carry dual citizenship. Despite the fact that Malaysia has instituted biometric screening programs as early as 1998, this agreement between these two neighbors was only solidified after a heavily armed, suspected terrorist group was detained in Southern Thailand with

[160] Bahukutumbi Raman, "Terrorism in Southern Thailand: An Update," *South Asia Analysis Group* Paper, no. 1501 (15 October 2005), http://www.southasiaanalysis.org/%5Cpapers16%5Cpaper1501.html (accessed 27 September 2010).

substantial sums of Malaysian currency.[161] While it may not be apparent to many states as they implement biometric programs, screening processes are heavily dependent on having accurate and shared data on perpetrators. Increased cooperation with neighboring states and the international community is crucial to have a successful screening program.

Despite the large numbers of incidents in Thailand within this "Unk/Other Included" dataset, it is important to note that nearly all of the other states exhibited perceptible decreases in terrorist incidents throughout the time period even when including "Unk/Other" perpetrators. Also in comparing the two datasets, eliminating the "Unk/Other" perpetrators from the dataset nearly eliminates all the recent activity within Thailand (similar to the situation in Pakistan above.) The large disparity between these two datasets that is evident only within Pakistan and Thailand is obviously related to perpetrator identity and may indicate some problems beyond border control or internal conflicts within these states. In addition to the problems of identifying perpetrators in the midst of such a large number of overall events within this state, the overwhelming number of "Unk/Other" incidents may indicate other deficiencies that may be on the side of the state or possibly the terrorist organizations. Looking at the states, these disparities may stem from a lack of counterterrorism investigation capabilities or agencies. On the other hand, if these "Unk/Other" events are truly terrorist activities, it could also be indicative of a lack of media capitalization on the part of terrorist organizations within these two states. While it is not possible to determine the exact reasoning for the large number of "Unk/Other" events within these two countries, there seems to still be perceptible trend data that can be analyzed with respect to biometric screening.

Turning to the "Unk/Other Excluded" dataset, there are again a smaller number of overall incidents all committed by what may be considered "known" groups. Overall, there is again a decreasing trend in terrorist incidents that decreases to zero after the transition period. In this dataset, it is reasonable to address each indecent that occurred since the inception of biometric borders to try to ascertain any individual relevance to

---

[161] "Malaysia–Thailand to use Biometric Identification to Check on Dual Citizenship," *The Star Online*, sec. Nation, 29 March 2007, http://www.thestar.com.my/news/story.asp?file=/2007/3/29/nation/20070329142754&sec=nation (accessed 27 September 2010).

biometric screening programs. Specifically, there are two attacks that took place during the transition period, which warrant investigation; one in Norway and one in Germany.

The attack in Norway was perpetrated by an individual against the Oslo Jewish Synagogue who apparently fired an automatic weapon at the structure in "the middle of the night."[162] Somehow, the authorities were informed that the synagogue was a "terrorist target" allowing an appropriate level of response so that ultimately no injuries were reported. Although there is little evidence that the perpetrator crossed a state border to conduct this attack, this event illustrates the fact the GTD perpetrator category labeled "Individual" may present some of the same difficulties as the "Unk/Other" category when attempting to determine if an attack fits this studies definition of an international incident.

The only incident within Germany after biometric screening was an attempted train bombing conducted by two individuals claiming to work for the terrorist organization Hizb al-Tahrir al-Islami (HT).[163] The perpetrators were legally in Germany as university students; the primary perpetrator had been in country since 2004, while the other entered the country on a student visa the same year of the attack. The primary perpetrator descended from a Lebanese family with known ties to Hizb al–Tahrir and interestingly, the perpetrator's father was under surveillance by the Lebanese government presumably from a time well before the individual applied for a German student visa.[164] Fortunately, during the attack, the bombs failed to explode and the authorities were able to capture and prosecute both individuals responsible. The primary perpetrator was arrested after attempting to flee back to his home in Lebanon and the other turned himself in after prompting by his reputable Lebanese family.[165] Although this attack failed due

---

[162] GTD dataset event ID# 200609170015.

[163] GTD dataset event ID# 200607310006. This group is active throughout the Middle East, China, and Russia – but little evidence of their existence in Germany. Global Security, "Hizb Ut-Tahrir Al-Islami (Islamic Party of Liberation)," http://www.globalsecurity.org/military/world/para/hizb-ut-tahrir.htm (accessed 09 June 2010).

[164] Gunter Latsch and others, "Terrorism in Germany: Every Investigator's Nightmare," *Spiegel Online International*, sec. International Terrorism, 28 August 2006, http://www.spiegel.de/international/spiegel/0,1518,433839,00.html.

[165] Jeffrey Fleishman, "Germany Startled to Find it's A Terror Target," *Los Angeles Times*, sec. The World, 19 August 2006 (accessed 17 September 2010).

to the ineptitude of the attackers to successfully ignite their devices, it illustrates some key issues with biometric screening programs and the importance of incorporating all available information into the screening process.

In contrast to some of the other attacks in the transition or post-biometric periods, this incident in Germany is a good representation of an attack that most likely originated externally to the state in question. While this example closely represents the type attacks that biometric screening is intended to thwart, it also illustrates some of the problems facing biometric screening programs. Specifically, this attack shows that biometric screening may be largely ineffective against: (1) individuals already in place who do not subsequently transit borders; and (2) individuals without any previous terrorist or criminal records that can be used in screening. It follows that terrorist organizations may seek to circumvent biometric screening programs by using individuals who are either already "in place" or individuals who have clean records that facilitate travel into the target state.

The single unsuccessful attack in Germany during the transition period helped to solidify the call for fully integrating all available terrorist and criminal information into state databases to better facilitate biometric screening programs (much like HSPD-6 in the U.S.)[166] It is important to note that Germany and other EU states are still in the process of building and expanding their biometric databases and screening processes through upgrades to the Second Generation Schengen Information System (SIS II.)[167] Despite the lack of a fully integrated and functional biometric screening process within the EU, there are still a few examples of successes that have occurred in recent years. One of the most notable German screening success occurred in 2008 when officials foiled a significant plot formulated by the Islamic Jihad Union after discovering documented

[166] Latsch and others, *Terrorism in Germany: Every Investigator's Nightmare*.

[167] European Commission, *Report from the Commission to the European Parliament and the Council on the Development of the Second Generation Schengen Information System (SIS II)* (Brussels: EU, 05 July 2010), 6, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0221:FIN:EN:PDF (accessed 27 September 2010).

travel by certain individuals into and out of Pakistan.[168] As the EU states get better at sharing and fusing information, there should be continued successes during the screening process associated with visa issuance and at border points of entry throughout the EU.

As suspected at the onset of this analysis, screening procedures during the transition period will include a mixture of biometric and non-biometric screening due to the amount of time required to fully transition systems and documents over to the new biometric requirements. One potential consideration is whether or not the defined duration of the transition period accurately reflects individual state implementation procedures (should it be longer/shorter or even individualized when comparing different states.) While this study used a predetermined and fixed time period for all states, follow on studies might consider assessing individual states with respect to their program implementation and hence tailor the transition period to each individual state. The bottom line is that during this transition period despite the duration, there remains a specified period of time where individuals may still have the ability to enter a country without being subject to biometric screening and hence countries are not reaping the full benefit of biometrically enabled screening processes. As such, most biometric screening programs and the resulting border control should be considered to be relatively porous during the transition period. This is mainly due to the ability of individuals to use previously issued documents to travel into a target state.

For the states that instituted biometric screening programs in 2005, moving past the transition period and assessing the post-biometric period is not entirely possible with the GTD dataset. Assessing the post--transition period is limited to only the events that occurred in 2007 since the GTD data ends at this point. Without additional data formatted in a similar fashion as the 1991–2007 GTD data, inferences beyond the transition period in these states only give a very limited view of the post-biometric period. Although it should be clear that assessing the data within these states in 2007 is far from conclusive, it is notable that there are no known attacks in any of the states (with

[168] Office of the Coordinator for Counterterrorism, "Country Reports on Terrorism 2008 Chapter 6– Terrorist Organizations," (2009), http://www.state.gov/s/ct/rls/crt/2008/122449.htm (accessed 09 June 2010).

the exception of the Thailand "Unk/Other Included" dataset.) Forecasting the longer-term trends for terrorism in these countries will depend on gathering and processing follow-on terrorist incident data as it relates to biometric screening in the same manner as was conducted in this study.

### 4. 2006—Austria, Denmark, France, Japan, Portugal, Singapore, UK, U.S.

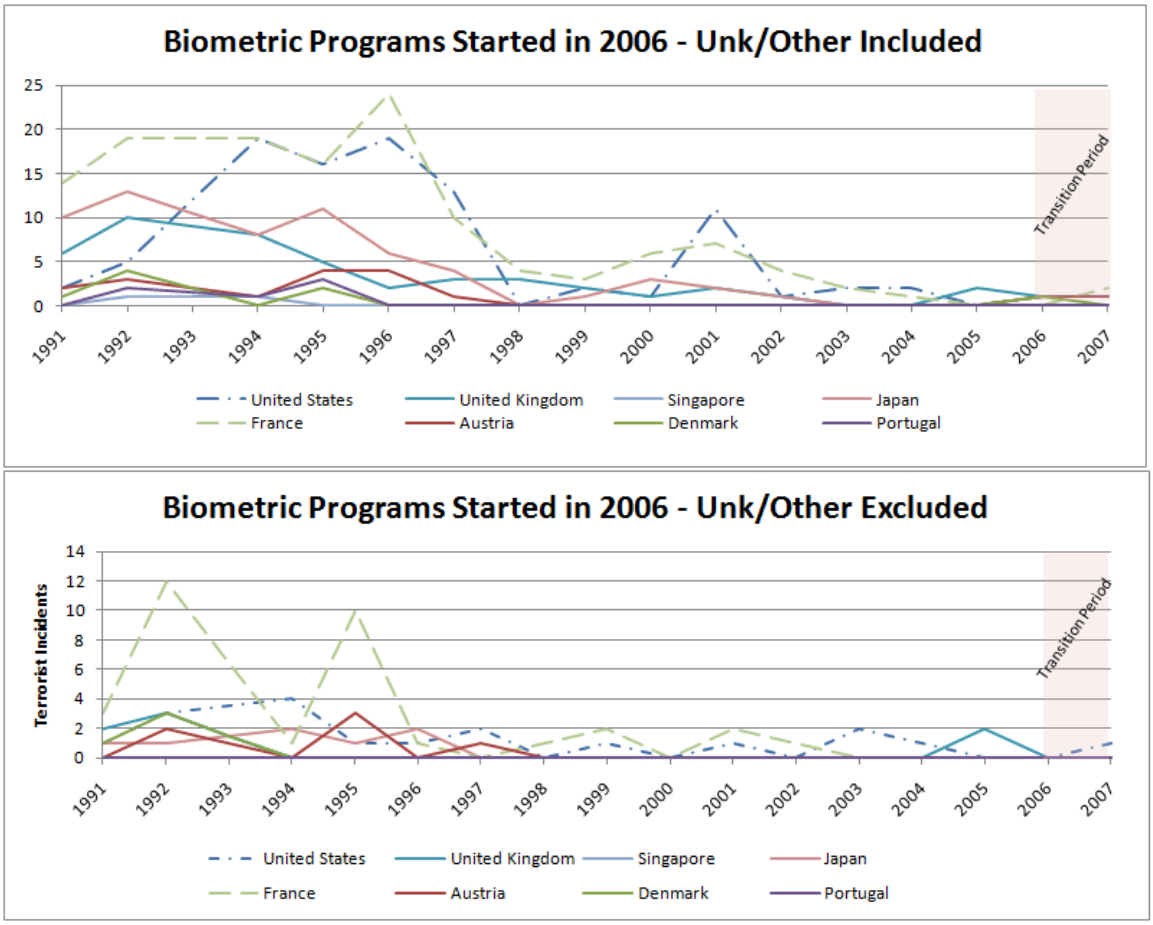



Figure 9. Biometric Screening—2006 Start Date.

States that implemented biometric screening programs in 2006 marked the last group included in this specific study. Most of these states were implementing screening programs aimed at incorporating the minimum requirements using the available e-Passport technology standards (mainly including digital facial photographs onto travel machine readable visas.) The U.S. and the states in EU, however, were implementing

substantially more intricate systems that combined multiple levels of biometric screening capabilities and information sharing. Some of these programs provided for extensive data sharing capabilities both within and externally to the state in question. Some components of these state programs are broken into individual elements that are solely based on identity verification and screening such as the US–VISIT and EURODAC programs.[169]

Another important distinction within this group is the fact that the U.S. and the UK had previously initiated some forms of biometric screening for immigrants. Specifically, in the U.S., digital fingerprints were being incorporated into the screening process as early as 2002. Unfortunately, these early attempts at biometric screening were not as productive due to the lack of a globalized standard for the data format and limited information sharing. Most of the early programs did not have the capacity for the required information sharing between internal or external state agencies to accurately screen immigrants. The lack of effective integration and information sharing within and between states is one of the main difficulties that prevented some of the early biometric screening initiatives from gaining ground and is still costing some states from maximizing their programs. The U.S. and EU move to consolidate terrorist screening into a centralized process using electronic media and biometrically searchable databases, paved the way for collaboration and integration with several other states.

Analyzing the activities that occurred in this group of states, there is again an initial decrease in the mid 1990s and then fairly steady numbers of incidents throughout the rest of the period. The transition period exceeds the available data within the GTD, but it is interesting to note that in the "Unk/Other Excluded," the U.S. was the only state to experience an incident after implementing biometric screening, an event that occurred one year after fully implementing biometric screening measures and fully integrated state databases. There is also less of a discrepancy between the two datasets within this group

[169] United States Visitor and Immigrant Status Indicator Technology (US–VISIT) and European Dactyloscopy (EURODAC) are examples of state specific programs that focus primarily on biometric identification and verification. Baldaccini, *Counter-Terrorism and the EU Strategy for Border Security: Framing Suspects with Biometric Documents and Databases*, 31; U.S. Dept of Homeland Security, *US–VISIT Biometric Identification Services*.

of states, and both datasets indicate the same general trends of a decreasing number of events in the limited biometric periods that are able to be analyzed on these charts.

In the "Unk/Other Included" dataset, Austria had a single incident and France had two separate incidents perpetrated by "Unknown" groups in the transition period. The incident in Austria was an arson event against a Turkish cultural site in Vienna in which there were no recorded injuries.[170] As with earlier "Unk/Other" incidents, it seems likely that this could be perpetrated by a group within Austria that is merely disgruntled with the cultural implications of the targeted site. The incidents in France, however, appear to be quite a bit larger in magnitude and are more in-line with what one would expect of an international incident. One incident was a string of bombings in the Basque region, which damaged several properties.[171] Although this attack was a larger magnitude, there is a large presence of separatist Basques within and around this region that have traditionally claimed similar attacks, so again this single event may still be indigenous to the Basque region. The other French attack, which occurred in 2007, was a parcel bomb sent to a law firm and former work place of President Nicholas Sarkozy, which ultimately killed one person and injured five others.[172] A Frenchmen was detained shortly after the blast for questioning, but a verdict or determination has yet to be released on whether or not he is responsible. Despite the magnitude of the attacks in France, current information sheds some doubt on either of these incidents being perpetrated by an external actor. Assuming that each of these incidents may have been committed by internal or indigenous perpetrators, there would be no incidents within these states after the inception of biometric screening.

Analyzing the "Unk/Other Excluded" dataset also yields similar results. In this dataset of "known" perpetrators, the U.S. was the sole state that experienced an incident again occurring during the transition period. The U.S. incident was the attempted bombing of the Mexican Consulate in New York by a lone individual using a fabricated

---

[170] GTD dataset event ID# 200711040002.

[171] GTD dataset event ID# 200704180006.

[172] GTD dataset event ID# 200712060001. Laure Bretton and Brian Rohan, "One Killed in Paris Parcel Bomb Blast," *Reuters*, sec. World, 06 December 2007, http://uk.reuters.com/article/idUKL067027520071206 (accessed 27 September 2010).

hand grenade.[173] It is suspected that this incident was perpetrated by an individual but there is not any information yet as to the suspect's origin or any publicized claims from known terrorist affiliates. This incident again illustrates the difficulty of the "Individual" term within the GTD dataset, as it nearly equates to the same characteristics as the "Unk/Other" perpetrator groups. It was also noted that the circumstances surrounding this specific attack appear nearly identical to an earlier incident performed by an individual on a bicycle, ultimately suspected to be a local employee.[174] Without further information on the suspect and according to our classification of events in this study, it is not possible to eliminate this event from the dataset, nor is it possible to evaluate the role of biometric screening in relation to this incident. Despite the difficulties in classifying terrorist incidents within the GTD dataset, it seems again evident that there are fewer events being committed during the transition period than in the prebiometric period.

As mentioned earlier, the analysis of the relation of terrorist incidents to biometric screening initiatives within this specific group of states is somewhat limited by the inclusive events within the dataset. Efforts were made to compare other datasets in order to account for the 2008–2009 timeframe, but other events were not classified in the same manner as the GTD format, which made numerical comparisons not feasible. Incorporating further data with similar fidelity as the GTD dataset will provide more conclusive results on whether or not incidents will continue to follow the downward trend that is noticeable in the first year of the transition period of this group of states.

### 5. Overall Trends

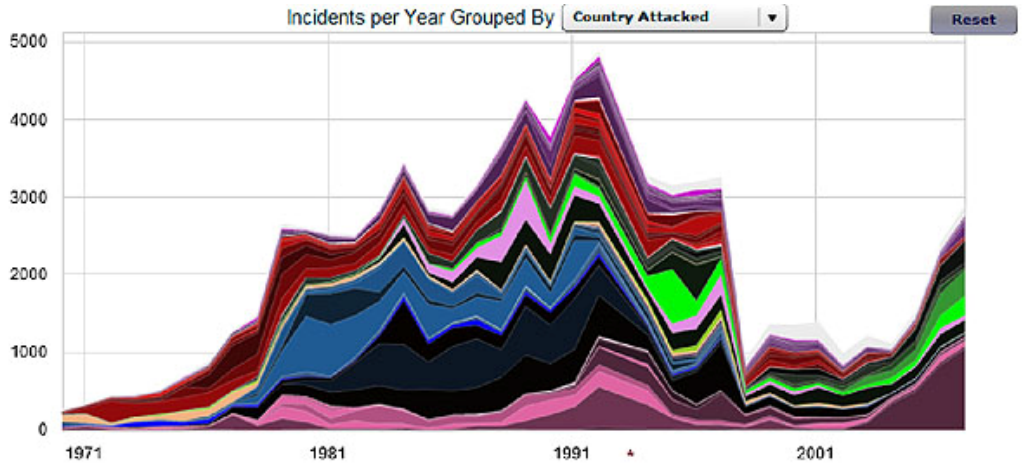
The graphical analysis of each state group that initiated biometric borders shows some important trends in terrorist incidents in the states that instituted biometric screening programs. Most importantly, the graphical analysis reaffirms the aggregated results and shows that states that have implemented biometric screening programs have

[173] GTD dataset event ID# 200710260003. Alison Gendar, Joe Gould and Jonathan Lemire, "Explosives Lobbed at Mexican Consulate," NY Daily News, http://www.nydailynews.com/news/2007/10/26/2007-10-26_explosives_lobbed_at_mexican_consulate.html (accessed 09 June 2010).

[174] Michelle Nichols, "Devices Explode at Mexican Consulate in New York," *Reuters*, sec. News, 26 October 2007, http://www.reuters.com/article/idUSN2636464720071026 (accessed 04 August 2010).

experienced both a decreasing trend of average annual incidents lower overall aggregate totals after implementing biometric screening programs. Analyzing the "Unk/Other Included" and the "Unk/Other Excluded" datasets separately allowed for analysis of information that could not be conclusively discounted. Despite the separation of each dataset, the trends tended to depict a decrease in incidents over the biometric time periods with the exception of Thailand and Pakistan.

One of the most obvious trends is the dramatic drop in incidents in the mid-1990s nearly across the spectrum of subject countries. The overall raw data from the GTD dataset without any manipulations also shows this decreasing trend that begins in the 1990s, this trend is fairly obvious when looking at the entire GTD dataset depicted in graphical form (including all known terrorist incidents across all states.)[175] Figure 10 shows all the terrorist incidents contained in the GTD prior to any manipulation for the purpose of this study in order to illustrate the drop in incidents that is clearly evident in the 1990s.




Entire GTD Dataset – all recorded terrorist activities from all countries.
[From http://www.start.umd.edu/gtd/ (accessed 01 June, 2010)]

Figure 10. Entire GTD Dataset—All Terrorist Activities (1971–2009).

[175] START - A Center of Excellence of the U.S. Department of Homeland Security, *Global Terrorism Database*.

This chart of the entire GTD dataset also depicts an increasing trend in incidents from 2001 to the present, but a large majority of that trend can be attributed to Iraq alone—with over 4000 incidents. As most of these incidents are related to the global war on terror, if they are discounted, terrorist incidents seem to follow a fairly steady trend. Contrasted with this steady trend, this studies aggregate and graphical analysis of the first 20 states to institute biometric screening shows that many of these states are enjoying a decreasing number of terrorist incidents after they instituted biometric screening programs. Additionally, the downward trend in terrorist incidents identified within many of these states appears to increase throughout the transition period and post-biometric period respectively, with fewer incidents occurring within states as biometric screening progresses. In the "Unk/Other Excluded" dataset, none of the states in this study have yet experienced an incident that could be positively attributed to a foreign group in the post-biometric period. Overall, the combined result of the aggregate and graphical analysis show that the first 20 states to implement biometric screening programs have experienced cumulative decreases in incidents perpetrated by "known" foreign perpetrators.

The most intriguing finding of this analysis is the distinct lack of incidents in the post-biometric period across the entire set of states. Of the first 20 states that have initiated biometric screening programs on or before 2005, none have yet suffered a terrorist attack by an external perpetrator in the post-biometric period (through the end of the GTD data.) Obviously, the last group of states is only one year from establishing a formal biometric program and not yet out of the transition period, so further analysis will be required to substantiate this finding. This certainly does not indicate that biometric screening is the single causal mechanism responsible for the lack of terrorist incidents in the post-biometric period, but it should prompt further quantitative analysis of biometric screening programs and their potential contribution to countering terrorism across international borders.

## D. CORRELATION ANALYSIS

Thus far, both the aggregate and graphical analysis illustrates that the institution of biometric screening programs coincides with a decrease in terrorist incidents during

both the transition and post-biometric periods in both datasets. Another method that may help to quantify or measure the strength of the relationship between biometric screening programs and terrorist incidents is to perform a statistical analysis of these two variables. Performing a statistical correlation between the biometric inception date and measured decreases in terrorist incidents for each of the states within our datasets should help measure the strength of the relationship and lay the ground work to conclusively attest that biometric screening is indeed an import tool in countering international terrorism.

### 1. Biometric Screening to Decreases in Terrorist Incidents

To investigate the correlation between biometric screening and decreases in terrorist incidents, this study will again consider both datasets and individually look at terrorist incidents before and after each states implemented biometric screening program. A statistical correlation will be conducted in order to assess the relationship between the number of annual terrorist incidents compared to the presence or absence of a biometric screening program based on the assumption that there will be cumulatively fewer annual terrorist incidents after biometric screening programs are put in place. For this method, states that experience fewer terrorist incidents after instituting biometric screening programs will exhibit stronger correlation scores. Measuring the strength of these relationships will allow for comparison across our sample of state as well as provide some evidence that a discernable and measureable relationship exists between biometric screening and decreases in international terrorist incidents.

### 2. Coding Dataset

The first correlation directly compares the average number of terrorist incidents per year in each state with the existence of a biometric screening program. An "annual" dummy variable was introduced for each state intended to represent the presence or absence of a biometric screening program ("1" = biometric screening program / "0" = no biometric screening program.) Using an annual basis to directly compare with the annual incident rates, states received a "1" beginning in the year after they implemented a biometric screening program and a "0" for the years before they instituted biometric

screening programs. The correlations between each states paired groupings of incidents and biometric program existence were run using S-Plus software.[176] With the variables coded in this manner, the expected results will be between "-1" and "1". Values between "-1" to a "0" would indicate the positive correlation between the presence of a biometric screening program and a decrease in terrorist activities. States with values closer to "-1" would have much fewer annual terrorist incidents after putting biometric screening programs in place. Positive values from "0" to "1" indicate that there were increases in annual terrorist incidents after instituting a biometric screening program. Essentially large negative numbers indicate a stronger correlation and further the hypothesis that the presence of a state biometric screening program corresponds with an overall reduced number of annual terrorist incidents.

| Correlation of Biometric Screening to Annual Terrorist Incidents "Unk/Other Included" | | | |
|---|---|---|---|
| 1998 | 2004 | 2005 | 2006 |
| Malaysia -0.5221 | Pakistan -0.0537 | Australia -0.3627 | Austria -0.0506 |
| | Belgium -0.4118 | Germany -0.2791 | Denmark -0.0296 |
| | D.Republic -0.3726 | New Zealand -0.3225 | France -0.2797 |
| | | Norway -0.1737 | Japan -0.2786 |
| | | Sweden -0.1392 | Portugal -0.1846 |
| | | Thailand 0.8179 | Singapore -0.2025 |
| | | Monaco N/A | UK -0.0221 |
| | | | U.S. -0.3074 |
| | | | Iceland N/A |
| Correlation of Biometric Screening to Annual Terrorist Incidents "Unk/Other Excluded" | | | |
| 1998 | 2004 | 2005 | 2006 |
| Malaysia 0.2091 | Pakistan -0.3244 | Australia -0.2091 | Austria -0.1541 |
| | Belgium -0.3328 | Germany -0.2503 | Denmark -0.1177 |
| | D.Republic N/A | New Zealand -0.1157 | France -0.2062 |
| | | Norway 0.0272 | Japan -0.2176 |
| | | Sweden -0.2142 | UK -0.1650 |
| | | Thailand -0.2988 | U.S. -0.1839 |
| | | Monaco N/A | Iceland N/A |
| | | | Portugal N/A |
| | | | Singapore N/A |

Table 12. Correlations of Screening to Annual Terrorist Incidents.

This correlation only considers those states that experienced some sort of terrorist incident during the 1991–2007 timeframe. Assessing the correlation results, it is immediately apparent that 30 of 33 individual cases indicated at least some correlation between the presence of a biometric screening program and a decrease in the annual number of terrorist incidents within the state. Although the preponderance of the

[176] Insightful Corp, *S-PLUS 8.0 for Windows*, Vol. B8052, 2007).

correlation data supports the hypothesis that biometric screening programs are coincident with decreases in annual terrorist incidents, there are some instances that merit discussion.

### 3. Correlation Outliers

The few states that did not show the expected correlation values were Malaysia and Norway in the "Unk/Other Excluded" dataset and Thailand in the "Unk/Other Included" dataset. These states exhibited correlation scores that indicated an increase in terrorist incidents after the implementation of biometric screening programs. The positive correlation in Malaysia and Norway both are partly due to the overall small number of events within these states, as well as the timing of the attacks. Both states had a relative absence of terrorist incidents before biometric screening implementation and then experienced a single incident after the inception of a biometric screening program. In each of these states, these events occurred during the transition period and neither has since experienced another incident through 2007. In this case, the positive correlation (or increase in terrorist incidents after biometric screening) seems more related to the timing of the event rather than truly representing any effect of biometric borders. In cases such as this, where there are so few incidents, examining each case might yield a more productive result.

The Thailand "Unk/Other Included" dataset is also showed a very strong positive correlation indicating that there was a marked increase in terrorist incidents after the state instituted biometric screening in 2005. It is again difficult to draw conclusions from this dataset due to the fact that 90% of the incidents within this dataset were perpetrated by "Unk/Other" actors and may or may not have any relation to biometric screening. It is also very likely that the recent internal political issues and the growing insurgency in Thailand may also be partly responsible for this correlation. Thailand experienced one of the most drastic increases in events in this dataset, going from two incidents in 2003 to 219 in 2007. On the other hand, the results from the Thailand "Unk/Other Excluded" dataset correlation appears more in line with the predicted hypothesis and shows that incidents perpetrated by "known" external terrorist groups begin to slightly decline after

Thailand instituted biometric screening programs. While there are an overwhelming number of incidents perpetrated by "Unk/Other" actors within Thailand, and overall terrorist incidents are on a recent upwards trend, it can be said that incidents by known perpetrators that originated externally to the state have declined after implementing biometric screening.

Overall, these results further confirm that the presence of biometric screening is coincident with reduced annual averages of international terrorist incidents within nearly all of the states in this study. Although the correlation scores for most states tend to be somewhat weak, they still offer evidence of the suspected trend and further reinforce the idea that biometric screening may be a contributor to decreasing terrorist incidents within these countries. One obvious conclusion that can be drawn from the presence of a weak correlation (as opposed to a stronger correlation) is that biometric screening is most likely not the only factor that influences decreases in terrorist incidents. Judging the overall statistical weight of the correlation values must also be put into context with the realization that none of these states have experienced any incidents in the post-biometric period using the GTD data from 1991–2007. The distinct lack of any international terrorist incidents conducted by known perpetrators in the post-biometric period is perhaps the most important finding of this study a fact that certainly appears to support the merit of biometric screening as part of a comprehensive program aimed at countering or deterring international terrorism.

## E. RESULTS

This thesis shows that in the analysis of the first 20 states to adopt biometric screening programs, almost every state has seen marked decreases in terrorist incidents conducted by known foreign individuals who would have crossed a border to perpetrate the attack. It further illustrates perceptible correlations between biometric screening programs and decreases in terrorist incidents (both perpetrated by known and "Unk/Other" individuals) within almost every state. Assessed as a whole, the graphical and statistical analysis of the GTD data leads to three different findings with respect to biometric screening programs. First, annual averages of terrorist incidents have

decreased over the three defined biometric periods for 19 out of 20 states. Second, no states have experienced any incidents in the post-biometric time period. Finally, there is a discernable correlation between the presence of a biometric screening program and a decrease in terrorist incidents.

From the graphical analysis, the finding of greatest relevance to biometric screening programs is the incident free post-biometric screening period. The observed decrease in incidents over the defined periods also reinforces the idea that it may take a certain amount of time after the implementation of a biometric screening program to develop a fully functioning and coherent system. Although the time periods outlined here were based on the anticipated fielding of equipment and the amount of time thought necessary to perceive tangible benefits, this study has illustrated that the use of specific time periods should be considered for use in assessing biometric screening programs. While this analysis produced some interesting findings, they are somewhat limited with respect to time as the GTD dataset only extends to 2007. Further analysis of terrorist incident data from 2007 to present is necessary in order to further substantiate these findings (assuming it can be similarly formatted and processed.) In spite of these limitations, these results should provide a foundation for future research in order to accurately assess the contributions of biometric screening at increasing state security and countering international terrorism.

The correlation of biometric screening programs with aggregate numbers of terrorist incidents is also significant since it demonstrates the existence of a distinct connection between these two variables. This approach can be further refined to isolate biometric screening from the other programs aimed at countering terrorism and perhaps more effectively measure the individual contributions of biometric screening programs. Revealing the correlation between biometric screening and numbers of terrorist incidents begins to illustrate that inherent ties may exist between these two variables and is one step further towards investigation of causation. These connections certainly do not imply that biometric screening programs are solely responsible for the noted reductions in terrorist incidents; it should be obvious that biometric screening is simply another tool

with the potential to contribute towards this goal. Further case studies, investigation of foiled plots and reassessment as data builds will all be necessary to determine the full extent of deterrence from biometric screening.

While this study is not meant to be a standalone analysis of biometric screening initiatives, it does numerically reinforce the notion that biometric screening is an important tool that states should use in conjunction with local law enforcement, intelligence and robust legal systems to improve counter terrorism efforts. Ensuring verifiable identity and conducting biometric screening is one step in the process of countering terrorism within state borders. Despite the fact that biometric screening programs are relatively young and the dataset is somewhat limited with respect to currency of events, these findings should certainly encourage the continuation of biometric screening initiatives and the development of methods to measure their effectiveness in countering international terrorism. Further analysis will be required as more states put biometric identification and screening initiatives in place and the programs themselves develop and mature.

# V. CONCLUSIONS

This thesis endeavored to provide a comprehensive assessment of biometric identification, as it pertains to border security and counter terrorism. It combined the readily available information on biometric identification with the practical applications currently used in immigration and border control in order to analyze the contributions of biometric identification to state security efforts. Accurately assessing the effectiveness of biometric borders will determine their prevalence within society—as such, this thesis has laid the foundations for quantifying the counter terrorism contributions of biometric identification systems. Ultimately, this work shows that there is a definite potential for states to achieve real security gains by incorporating biometrics into border control programs and state screening mechanisms.

## A. BIOMETRICS IN VERIFABLE IDENTITY

Biometric identifiers have very unique characteristics, are proprietary to every individual, can be difficult to falsify, and are proving to be highly reliable for identity verification and screening. The ability to rapidly and reliably ascertain an individual's identity is undoubtedly becoming an important state security tool. As states realize tangible security benefits from biometric identification programs, many are demanding that verifiable identity be provided at their borders. In addition to biometric identification becoming the norm throughout the international community, several states are seeking corresponding screening programs to enhance state security. As states implement biometric identifiers into an increasing number of identification programs, particular attention needs to be placed on understanding the underlying principles of how the identifiers will be used in order to maximize their results. States should be cognizant of the methodology and constraints that underlie biometric technologies in order to develop efficient and accurate identification systems. As verifiable identity becomes more readily available, states also need to consider information integration and sharing in order to maximize the security measures that are afforded by biometric identification systems.

## B. ASSESSMENT RESULTS

In an effort to quantify the role of biometric identification in state security; this thesis investigated two distinct biometric initiatives. The first was an analysis of the U.S. visa refusals with respect to the biometric identification initiatives associated with US–VISIT and the integrated databases under HSPD–6. The second and more substantial assessment was intended to evaluate the contributions of biometric identification programs at reducing the number of foreign perpetrated terrorist incidents within a state. These assessments both indicated that biometric identification and enhanced screening can bolster state security and may protect against international terrorist incidents.

### 1. Screening Effectiveness

Screening individuals throughout the immigration process is beginning to take on a much larger importance than ever before and many states have developed biometric identification systems in order to accomplish this goal. These systems can detect fraudulent identities, highlight known actors, or assist in prosecution efforts. Assessing the U.S. visa refusals was an effort to investigate the potential contributions of these state specific biometrically based screening initiatives.

As suspected, it appears that U.S. screening enhancements made after 9/11 have significantly improved the ability to determine the acceptability of an intending immigrant. Judging both from reported successes as well as the numerical analysis of U.S. visa refusals, it is clear that the U.S. has improved the ability to deny a larger percentage of U.S. applicants on the basis of security and terrorism concerns. This is largely due to the improved biometric identification and screening capabilities imposed after 9/11 through US–VISIT and HSPD–6. These results are specific to the U.S. but have applicability to other states currently in the process of instituting similar screening mechanisms. As these programs are increasingly refined and identifiers more commonly shared between states, immigration and border control programs will continue to see similar gains in preventing access to unwarranted individuals.

### 2. Biometric Borders Vs. Terrorism

Measuring the effectiveness of biometric identification against terrorism as a whole is a difficult task and receives little attention in the way of large-scale studies. This thesis attempted to lay the foundation for a scholarly debate as to the effectiveness of state biometric identification programs and their role in countering international terrorism. Biometric borders are a relatively new phenomenon and state specific screening procedures are still being developed, yet already there seems to be substantial merit. Focusing on international terrorism, this thesis also found that of the first 20 states to implement biometric identification programs, nearly every one experienced documented decreases in terrorist activity conducted by foreign nationals within their borders. These decreases were immediate, perceptible, and positively correlated to the presence of a biometric program. More importantly, none of the states has experienced an incident by a known foreign perpetrator in the post-biometric period. Although this assessment had some documented limitations due to the available data and duration, it substantially reinforces the idea that biometric identification may play a positive role in increasing state security against foreign national terrorist attacks.

### 3. Follow-on Research

This thesis has shown perceptible links between biometric identification and state security, yet there is ample room to improve this quantitative analysis. The GTD is only one of several terrorist datasets, while comprehensive, it is not exhaustive. Future efforts to quantify terrorist incidents may consider other separate databases to build upon this analysis. There is also room for the investigation of the numerous foiled terrorist plots with respect to biometric identification. Within the U.S. alone, the Heritage Foundation reports that to date, there have been 28 foiled terrorist plots.[177] Investigating the biometric screening implications of these attacks may provide further insights on whether or not biometrics played a role in any respect. Other potentially worthwhile endeavors

[177] Jena McNeill, "Detroit Terror Plot Makes 28 Plots Foiled since 9/11," *The Heritage Foundation* WebMemo #2741 (2009), http://www.heritage.org/Research/HomelandSecurity/wm2741.cfm (accessed 11 March 2010).

could be investigating biometric screening as it relates to those within our borders—obviously this brings up several civil rights concerns and ample fourth amendment questions that need to be adequately weighed and addressed.

## C. RECOMMENDATIONS

Surprisingly, much of the literature on biometric identification tends to critique and discourage the widespread implementation of biometrics in state security programs. On the contrary, this thesis has provided evidence that should encourage further development, integration, and analysis of biometric identification in state identification programs. Biometric identifiers offer substantial gains in solving the identity problem and can be applied in numerous ways to increase security. States not currently using biometric identification programs as part of a comprehensive security strategy should carefully reconsider the potential benefits of biometric identification. Similarly, internal state identification programs should explore the options that biometric incorporation could provide in strengthening verifiable identity and improving current screening functions.

Considering the readily available biometric travel documents and the perceptible security gains associated with e–Passport program, it is surprising that more states are not choosing to implement biometric identification. The results of this study, as well as the publicized successes of these programs, all suggest that states can achieve tangible security gains from merely complying with existing standards. The ability to share identification date will also become a premium and states need to consider agreements that will enable cooperative watchlisting. Creating an integrated system should leave little room for international criminals or terrorists to hide when attempting to transit state borders.

As biometric identifiers become further incorporated into state immigration and border control programs, there also seems to be a commensurate interest in national biometric identification programs. These localized efforts are aimed at improving internal state identification processes. The EU has undertaken efforts to create a biometrically enabled national ID card and the U.S. has been debating similar initiatives

through the REAL ID Act.[178] Based on the capabilities of biometric identifiers and their success when paired with appropriate systems, it seems that these initiatives should consider incorporating biometrics as a method of enhancing the reliability of state identification programs. In addition to enhancing verifiable identity, the ability to fuse information on wanted individuals should correspondingly lead to more effective law enforcement.

Overall, it seems that biometric borders are providing real security gains by allowing states to access and utilize verifiable identity. As these systems become further integrated and accuracies improve, the propensity for criminals and terrorists to advantage personal identity will be dramatically reduced. Biometric identification is only a small part of a comprehensive security strategy and needs to be seamlessly incorporated with other security measures. Aside from falsification, the next potential avenue that individuals may pursue to avoid biometric identification in accomplishing criminal or terrorist activities is illegal immigration or taking advantage of individuals with "trusted" identities. While it is near impossible to prevent the first–time offender, biometric offers states a much better system to track and record known individuals. The ability of states to leverage identity is another layer of security when it comes to protecting borders and ensuring state security.

[178] Janice Kephart, "Repealing REAL ID? Rolling Back Driver's License Security," *Center for Immigration Studies: Backgrounder* (June 2009), http://www.cis.org/realid (accessed 13 October 2009).

THIS PAGE INTENTIONALLY LEFT BLANK

# LIST OF REFERENCES


Ackleson, Jason. "Securing through Technology?"Smart Borders" After September 11th." *Knowledge and Policy; the International Journal of Knowledge Transfer and Utilization* 16, no. 1 (Spring 2003): 56.

Amoore, Louise. "Biometric Borders: Governing Mobilities in the War on Terror." *Political Geography* 25, no. 3 (01 February 2006): 336.

Ashbourn, Julian. *Practical Biometrics: From Aspiration to Implementation*. London; New York: Springer, 2004.

Avoine, Gildas, Kassem Kalach, and Jean-Jaques Quisquater. "EPassport: Securing International Contacts with Contactless Chips." In *Financial Cryptography and Data Security 12th International Conference, FC 2008*, edited by G. Tsudik. Berlin: Springer–Verlag, 2008.

Bajoria, Jayshree. "The Troubled Afghan–Pakistan Border." *Council on Foreign Relations* Backgrounders, (20 March 2009), http://www.cfr.org/publication/14905/troubled_afghanpakistani_border.html (accessed 09 August, 2010).

Baldaccini, Anneliese. "Counter-Terrorism and the EU Strategy for Border Security: Framing Suspects with Biometric Documents and Databases." *European Journal of Migration and Law* 10, no. 1 (January 2008): 31.

Ball, Kirstie and Frank Webster. *The Intensification of Surveillance: Crime, Terrorism and Warfare in the Information Age*. London: Pluto Press, 2003.

Barkakati, Nabajyoti and U.S. Government Accountability Office. *Border Security Improvements in the Department of State's Development Process could Increase the Security of Passport Cards and Border Crossing Cards*. Washington, DC: GAO 10-589, 2010, http://www.gao.gov/new.items/d10589.pdf (accessed 16 July 2010).

Bersani, Bianca, Paul Nieuwbeerta, and John Laub. "Predicting Trajectories of Offending Over the Life Course: Findings from a Dutch Conviction Cohort." *The Journal of Research in Crime and Delinquency* 46, no. 4 (2009): 468.

Bolle, Ruud M., Johathan H. Connell, Sharath Pankanti, Nalini K. Ratha, and Andrew W. Senior, eds. *Guide to Biometrics*. New York: Springer, 2004.

Bonner, David. "United Kingdom: The United Kingdom Response to Terrorism." *Terrorism and Political Violence* 4, no. 4 (1992): 171.

Bretton, Laure and Brian Rohan. "One Killed in Paris Parcel Bomb Blast." *Reuters,* 6 December, 2007, UK Edition, sec. World.

Chunovic, Louis. "Stopping Terrorist Travel: The Pre-Flight 253 View." *Government Security News* 8, no. 2 (01 February 2010): 1–23.

Clarke, Roger. "Human Identification in Information Systems: Management Challenges and Public Policy Issues." *Information Technology and People* 7, no. 4 (1994): 6–37.

CNN iReport. "Thai - Burma Border, Crossing for Food." http://www.ireport.com/docs/DOC-22600 (accessed 06 June 2010).

Daugman, John G. "High Confidence Visual Recognition of Persons by a Test of Statistical Independence." *IEEE Transactions on Pattern Analysis and Machine Intelligence* 15, no. 11 (1993): 1148.

Difo, Germain. *Ordinary Measures, Extraordinary Results: An Assessment of Foiled Plots since 9/11*. Washington DC: American Security Project, 2010, http://www.americansecurityproject.org/content/wp-content/uploads/2010/05/Foiled-Plots.pdf (accessed 01 June 2010).

Eldridge, Thomas R. *9/11 and Terrorist Travel Staff Report of the National Commission on Terrorist Attacks upon the United States*. Washington, DC: National Commission on Terrorist Attacks upon the United States, 2004, http://purl.access.gpo.gov/GPO/LPS53197.

European Commission. *Report from the Commission to the European Parliament and the Council on the Development of the Second Generation Schengen Information System (SIS II)*. Brussels: EU, 05 July 2010, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0221:FIN:EN:PDF (accessed 27 September 2010).

Find Biometrics. "Over 60+ Countries Now Issuing ePassports." *Security Document World* Articles, (30 December 2008): 04 June 2010, http://www.findbiometrics.com/articles/i/6390/ (accessed 04 June 2010).

Fleishman, Jeffrey. "Germany Startled to Find it's A Terror Target." *Los Angeles Times,* 19 August 2006, sec. The World (accessed 17 September 2010).

Ford, Jess T. and U.S. Government Accountability Office. *State Department Improvements Needed to Strengthen U.S. Passport Fraud Detection Efforts: Report to the Committee on Homeland Security and Governmental Affairs, US Senate*. Washington, DC: GAO-05-477, May 2005, http://www.gao.gov/new.items/d05477.pdf (accessed 10 August 2010).

Frittelli, John. *Transportation Security: Issues for the 109th Congress*. Washington D.C: Congressional Research Service, Library of Congress, July 2005, http://fpc.state.gov/documents/organization/52533.pdf (accessed 15 May 2010).

Garcia, Michael John and Ruth Ellen Wasem. *Immigration: Terrorist Grounds for Exclusion of Aliens*. Washington, DC: Congressional Information Service and the Library of Congress, May 2005, http://fpc.state.gov/documents/organization/48380.pdf (accessed 12 July 2010).

Garfinkel, Simson. *Database Nation: The Death of Privacy in the 21st Century*. Sebastopol, CA: O'Reilly, 2000.

Garvey, Martin and Eric Chabrow. "Border ID System First Part of $10B Effort." *Information Systems News* no. 971 (12 January 2004): 22, http://www.informationweek.com/story/showArticle.jhtml?articleID=17300298 (accessed 09 October 2009).

Gendar, Alison, Joe Gould, and Jonathan Lemire. "Explosives Lobbed at Mexican Consulate." NY Daily News. http://www.nydailynews.com/news/2007/10/26/2007-10-26_explosives_lobbed_at_mexican_consulate.html (accessed 09 June 2010).

Global Security. "Hizb Ut-Tahrir Al-Islami (Islamic Party of Liberation)." http://www.globalsecurity.org/military/world/para/hizb-ut-tahrir.htm (accessed 09 June 2010).

Gray, Myra. "Terrorism and New Biometrics Technologies." *Security Magazine* 45, no. 11 (01 November 2008): 80–81.

Hite, Randolph C. and U.S. Government Accountability Office. *Information Technology: Homeland Security Needs to Improve Entry Exit System Expenditure Planning*. Washington, DC: GAO-03-563, June 2003, http://www.gao.gov/new.items/d03563.pdf (accessed 19 January 2010).

Hosein, Ian. "Transforming Travel and Border Controls: Checkpoints in the Open Society." *Government Information Quarterly* 22, no. 4 (1 October 2005): 594–625.

Hsu, Spencer S. "U.S. Preparing to Drop Tracking of Foreigners' Departures by Land." *The Washington Post,* 2006, sec. 1.

———. "U.S. to Expand Immigration Checks to all Local Jails." *The Washington Post-,* 19 May 2009, sec. Politics.

Insightful Corp. *S-PLUS 8.0 for Windows*. Vol. B8052, 2007, http://spotfire.tibco.com (accessed 15 February 2010).

International Civil Aviation Organization. *Guidelines: Electronic Machine Readable Travel Documents & Passenger Facilitation*. 1st ed. Quebec, Canada: ICAO Secretary General, 2008, http://www.icao.int/icao/en/atb/meetings/2008/TagMRTD18/TagMrtd18_wp03.pdf (accessed 24 May 2010).

———. *Machine Readable Travel Documents: Specifications for Electronically Enabled Passports with Biometric Identification Capability*. 6th ed. Vol. 2, Doc 9303. Québec, Canada: ICAO Secretary General, 2006 (accessed 09 October 2009).

Jain, Anil K. "Fingerprints: Proving Ground for Pattern Recognition." Hong Kong, 2006.

———., Ruud Bolle, and Sharath Pankanti, eds. *Biometrics: Personal Identification in Networked Society*. New York: Springer Science+Business Media Inc., 1996.

Kean, Thomas H., and Lee Hamilton. *Report on the Status of 9/11 Commission Recommendations*. Washington, DC: 9/11 Public Discourse Project, 2005.

Kent, Stephen T., Lynette I. Millett, National Research Council (U.S.). Committee on Authentication Technologies and Their Privacy Implications and National Research Council (U.S.). Computer Science and Telecommunications Board. *IDs–Not that Easy: Questions about Nationwide Identity Systems*. Washington, D.C: National Academy Press, 2002.

Kephart, Janice. "Repealing REAL ID? Rolling Back Driver's License Security." *Center for Immigration Studies: Backgrounder* (June 2009), http://www.cis.org/realid (accessed 13 October 2009).

Kim, Won. "On US Homeland Security and Database Technology." *Journal of Database Management* 16, no. 1 (January–March 2005): 1.

Kosta, Eleni, Martin Meints, Marit Hansen, and Mark Gasson. "New Approaches for Security, Privacy and Trust in Complex Environments." In *IFIP International Federation for Information Processing*, edited by Hein Venter, Mariki Eloff, Les Labuschagne, Jan Eloff and Rossouw Von Solms. Vol. 232, 467–472. Boston: Springer, 2007.

Krouse, William J. *Terrorist Identification, Screening, and Tracking Under Homeland Security Presidential Directive 6 (HSPD–6)*. Ft. Belvoir: Defense Technical Information Center, 2004, http://handle.dtic.mil/100.2/ADA445120 (accessed 19 January 2010).

Lake, Jennifer E. *Border Security: The Complexity of the Challenge*. Washington, D.C: Congressional Research Service, Library of Congress, January 2007, http://www.fas.org/sgp/crs/homesec/RL32839.pdf (accessed 11 December 2009).

Latsch, Gunter, Guido Kleinhubbert, Cordula Meyer, Holger Stark, Daniel Steinvorth, Andreas Ulrich, and Marc Widmann. "Terrorism in Germany: Every Investigator's Nightmare." *Spiegel Online International,* 28 August 2006, English, sec. International Terrorism, http://www.spiegel.de/international/spiegel/0,1518,433839,00.html.

Li, Stan Z., Jianhuang Lai, Tieniu Tan, Guocan Feng, and Yunhong Wang, eds. *Advances in Biometric Person Authentication: 5th Chinese Conference on Biometric Recognition, SINOBIOMETRICS 2004, Guangzhou, China, December 13–14, 2004, Proceedings*. Berlin, Germany: Springer, 2004.

Lin, Hong and Jain K. Anil. "Integrating Faces and Fingerprints for Personal Identification." *IEEE Transactions on Pattern Analysis and Machine Intelligence* 20, no. 12 (01 December 1998): 10 November 2009, http://www.cse.unr.edu/~bebis/CS790Q/PaperPresentations/FaceFingerprintFusion.pdf (accessed 10 November 2009).

Lord, Kristin M. *The Perils and Promise of Global Transparency: Why the Information Revolution may Not Lead to Security, Democracy, Or Peace*. Albany: State University of New York Press, 2006.

M2 Presswire. "Ten Point Plan for Border Protection and Immigration Reform; First Milestone Met as Fingerprint Checks Go Global." *Normans Media Ltd,* 14 January, 2008, Coventry, sec. UK Government, http://proquest.umi.com/pqdweb?did=1412330111&Fmt=7&clientId=11969&RQT=309&VName=PQD (accessed 17 March, 2010).

"Malaysia–Thailand to use Biometric Identification to Check on Dual Citizenship." *The Star Online,* 29 March 2007, sec. Nation, http://www.thestar.com.my/news/story.asp?file=/2007/3/29/nation/20070329142754&sec=nation (accessed 27 September 2010).

McCabe, R. Michael and Elaine M. Newton, eds. *American National Standard for Information Systems - Data Format for the Interchange of Fingerprint, Facial, and Other Biometric Information - Part 1*. NIST Special Publication 500–271. Gaithersburg, MD: American National Standards Institute, Inc. May 2007.

McMunn, Mary K. "Machine Readable Travel Documents with Biometric Enhancement: The ICAO Standard." *ICAO MRTD Report* 1, no. 1 (2006): 22, http://www2.icao.int/en/MRTD/Pages/ICAOMRTDReport.aspx (accessed 24 May 2010).

McNeill, Jena. "Detroit Terror Plot Makes 28 Plots Foiled since 9/11." *The Heritage Foundation* WebMemo #2741, (26 December 2009): 11 March 2010, http://www.heritage.org/Research/HomelandSecurity/wm2741.cfm (accessed 11 March 2010).

Most, C. Maxine. "Biometrics and Border Control: Beyond US-VISIT." *Digital ID World* (20 January 2004): 04 March 2010, 18–21, http://magazine.digitalidworld.com/Sep04/Page18.pdf (accessed 04 March 2010).

National Consortium for the Study of Terrorism and Responses to Terrorism. *Global Terrorism Database Codebook 3.0*. College Park, MD: University of Maryland, 2009, http://www.start.umd.edu/gtd/downloads/Codebook.pdf (accessed 01 December 2009).

National Counterterrorism Center. *2009 Report on Terrorism*. Washington, DC: National Counterterrorism Center, 2010, http://www.nctc.gov/witsbanner/docs/2009_report_on_terrorism.pdf (accessed 07 August 2010).

Nichols, Michelle. "Devices Explode at Mexican Consulate in New York." *Reuters,* 26 October 2007, U.S. Edition, sec. News, http://www.reuters.com/article/idUSN2636464720071026 (accessed 04 August 2010).

Niksch, Larry. *Abu Sayyaf: Target of Philippine–U.S. Anti-Terrorism Cooperation*. Washington D.C: Congressional Research Service, Library of Congress, 2002, http://www.fas.org/irp/crs/RL31265.pdf (accessed 04 August 2010).

Noble, Ronald K. "Opening Remarks: 5th INTERPOL International Symposium on Fingerprints." Lyon, France, INTERPOL, 04 June 2008, http://www.interpol.int/public/ICPO/speeches/2008/SGFingerprints20080604.asp# (accessed 01 October 2010).

North, David. "At DHS, Perps have Rights that Citizens Don't." Center For Immigration Studies. http://www.cis.org/north/perps-have-rights (accessed 08 May 2010).

O'Brien, Luke. DHS Biometric Program in Trouble. *Wired,* 26 February 2007, http://www.wired.com/science/discoveries/news/2007/02/72792 (accessed 22 January 2010).

Office of the Coordinator for Counterterrorism. "Country Reports on Terrorism 2008 Chapter 6–Terrorist Organizations." (2009): 09 June 2010, http://www.state.gov/s/ct/rls/crt/2008/122449.htm (accessed 09 June 2010).

Paulus, Sachar, Norbert Pohlmann, and Helmut Reimer, eds. *ISSE 2006 - Securing Electronic Business Processes*. Wiesbaden, Germany: Vieweg (GWV), 2006, http://www.springerlink.com/content/g075k556151058n1/fulltext.pdf (accessed 26 May 2010).

Raman, Bahukutumbi. "Terrorism in Southern Thailand: An Update." *South Asia Analysis Group* Paper, no. 1501 (15 October 2005), http://www.southasiaanalysis.org/%5Cpapers16%5Cpaper1501.html (accessed 27 September 2010).

Rhodes, Keith A. and U.S. General Accounting Office. *Information Security Challenges in using Biometrics*. Washington, D.C: GAO-03-1137T, September 2003, http://www.gao.gov/new.items/d031137t.pdf (accessed 17 February 2010).

Rhodes, Keith A. and Gregory C. Wilshusen. *Information Security: Homeland Security Needs to Immediately Address Significant Weaknesses in Systems Supporting the US-VISIT Program: Report to Congressional Requesters*. Washington, D.C: GAO-07-870, July 2007, http://www.gao.gov/new.items/d07870.pdf (accessed 12 July 2010).

Safir, Howard and Peter Reinharz. "DNA Testing: The Next Big Crime-Busting Breakthrough." *City Journal* Winter 2000, http://www.city-journal.org/html/10_1_dna_testing.html (accessed 15 May 2010).

Schaeffer, Richard C. *CNSS Instruction no 4009: National Information Assurance (IA) Glossary,* Committee on National Security Systems, 2010, http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf (accessed 01 October 2010).

Schmid, Alex Peter and A. J. Jongman. *Political Terrorism: A New Guide to Actors, Authors, Concepts, Data Bases, Theories, & Literature*. New Brunswick, N.J: Transaction Publishers, 2005.

Schneier, Bruce. *Beyond Fear: Thinking Sensibly about Security in an Uncertain World*. New York: Copernicus Books, 2003.

Seghetti, Lisa M. and Stephen R. Viña. *U.S. Visitor and Immigrant Status Indicator Technology (US–VISIT) Program*. Washington, D.C: Congressional Research Service, Library of Congress, January 2006, http://www.usembassy.it/pdf/other/RL32234.pdf (accessed 09 December 2009).

Sobieck, S. M. "Democratic Responses to International Terrorism in Germany." *Contributions in Political Science.* 340, (1994): 43.

START - A Center of Excellence of the U.S. Department of Homeland Security. "Global Terrorism Database." University of Maryland. http://www.start.umd.edu/gtd (accessed 01 December 2009).

Tistarelli, Massimo, Josef Bigün, and Enrico Grosso, eds. *Advanced Studies in Biometrics: Summer School on Biometrics, Alghero Italy, June 2003, Revised Selected Lectures and Papers*. Berlin, Germany: Springer, 2005.

Tkacik, John J. Jr. "Why the Department of Homeland Security should Control Visas." *The Heritage Foundation* Backgrounder, no. 1569 (12 July 2002): 8 March 2010, http://www.heritage.org/Research/HomelandSecurity/BG1569.cfm#pgfId-998924 (accessed 08 March 2010).

U.S. Dept of Commerce. "Office of Travel & Tourism Industries." U.S. Department of Commerce. http://tinet.ita.doc.gov/view/m-2008-I-001/table1.html (accessed 14 December 2009).

U.S. Dept of Homeland Security. "Enhancing Security through Biometric Identification." U.S. http://www.dhs.gov/xlibrary/assets/usvisit/usvisit_edu_biometrics_brochure_english.pdf (accessed 17 February 2010).

———. "Government Agencies using US–VISIT." U.S. http://www.dhs.gov/files/programs/gc_1214422497220.shtm (accessed 17 October 2009).

———. *Immigration Enforcement Actions: 2009*. Washington, DC: Office of Immigration Statistics, 2009, http://www.dhs.gov/xlibrary/assets/statistics/publications/enforcement_ar_2009.pdf.

U.S. Department of Justice. *Follow Up Audit of the Terrorist Screening Center*. Washington, DC: Audit Report 07–41, Office of the Inspector General, Audit Division, September 2007, http://www.justice.gov/oig/reports/FBI/a0741/final.pdf (accessed 11 August 2010).

———. "US-VISIT Biometric Identification Services." US. http://www.dhs.gov/files/programs/gc_1208531081211.shtm (accessed 09 December 2009).

U.S. Dept of State. "Visa Statistics: Report of the Visa Office." http://www.travel.state.gov/visa/statistics/statistics_1476.html (accessed 14 October 2010).

———. "Visa Waiver Program (VWP)." U.S. http://travel.state.gov/visa/temp/without/without_1990.html (accessed 03 June 2010).

———. "Worldwide Non-Immigrant Visa Issuances Fiscal Years 2003–2008." U.S. Dept of State. http://www.travel.state.gov/visa/frvi/statistics/statistics_4399.html (accessed 14 December 2009).

U.S. Joint Forces Command. *The JOE, Joint Operating Environment, 2008 Challenges and Implications for the Future Joint Force*. Suffolk, VA: United States Joint Forces Command, Center for Joint Futures, 2008, http://www.jfcom.mil/newslink/storyarchive/2008/JOE2008.pdf (accessed 2 February 2010).

United States. *Homeland Security Presidential Directive/HSPD–6 Integration and use of Screening Information*. Washington, D.C: White House, Office of the Press Secretary, 16 September 2003, http://www.dhs.gov/xabout/laws/gc_1214594853475.shtm#1.

United States Congress. *Omnibus Consolidated Appropriations Act, 1997*. Washington, DC: U.S. Congress, 1996.

Wasem, Ruth Ellen. *Immigration Visa Issuances and Grounds for Exclusion Policy and Trends*. Washington, D.C: Congressional Research Service, Library of Congress, March, 2010.

Watner, Carl and Wendy McElroy. *National Identification Systems: Essays in Opposition*. Jefferson, NC: McFarland & Co, 2004.

Wayman, James L. "Error Rate Equations for the General Biometric System." *Robotics & Automation Magazine, IEEE* 6, no. 1 (1999): 35–48.

Woodward, John D. Jr. "Using Biometrics to Achieve Identity Dominance in the Global War on Terrorism." *Military Review* 85, no. 5 (Sep/Oct 2005): 30.

Zeb, Rizwan. "Cross Border Terrorism Issues Plaguing Pakistan-Afghanistan Relations." *China and Eurasia Forum Quarterly* 4, no. 2 (2006): 69, http://www.silkroadstudies.org/new/docs/CEF/Quarterly/May_2006/Zeb.pdf (accessed 29 July 2010).

Zill, Oriana. "Crossing Borders: How Terrorists use Fake Passports, Visas, and Other Identity Documents." *Frontline Reports* (2010), http://www.pbs.org/wgbh/pages/frontline/shows/trail/etc/fake.html (accessed 10 August 2010).

THIS PAGE INTENTIONALLY LEFT BLANK

# INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California