Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
SEP 2006		**00-09-2006 to 00-09-2006**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Radicalization. Homeland Security Implication	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Rand Corporation,1776 Main Street,PO Box 2138,Santa Monica,CA,90407-2138**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

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

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**		**8**	

TESTIMONY

Radicalization

Homeland Security Implication

JOHN D. WOODWARD, JR.

CT-267

September 2006

Testimony presented to the House Homeland Security Committee, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment on September 20, 2006

Published 2006 by the RAND Corporation
1776 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138
1200 South Hayes Street, Arlington, VA 22202-5050
4570 Fifth Avenue, Suite 600, Pittsburgh, PA 15213
RAND URL: http://www.rand.org/
To order RAND documents or to obtain additional information, contact
Distribution Services: Telephone: (310) 451-7002;
Fax: (310) 451-6915; Email: order@rand.org

John D. Woodward, Jr.[1]
The RAND Corporation

Radicalization: Homeland Security Implication

Before the Committee on Homeland Security
Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment
United State House of Representatives

September 20, 2006

Introduction

Good afternoon. I thank the distinguished Chairman, Ranking Member, and Members of this Subcommittee for inviting me to testify about homeland security challenges, with particular reference to how the U.S. Government can make better use of biometric technologies to protect the nation, in a manner consistent with American civil liberties. I base my testimony on my RAND research as well as my experience from 2003 to 2005 as Director of the Department of Defense Biometrics Management Office, the organization responsible for planning, coordinating, and implementing the Department's biometric activities.[2]

Today, I want to make two basic points with respect to biometrics, which are automated methods of recognizing a person based on a physiological or behavioral characteristic:

1. The U.S. Government is currently using biometric technologies in various ways to make the nation safer.
2. We can and should make better use of these technologies for homeland security purposes.

Current Use

With respect to current U.S. Government use, it is well established that biometric technologies are a significant tool contributing to homeland and national security. They are a significant tool

---

[1] The opinions and conclusions expressed in this testimony are the author's alone and should not be interpreted as representing those of RAND or any of the sponsors of its research. This product is part of the RAND Corporation testimony series. RAND testimonies record testimony presented by RAND associates to federal, state, or local legislative committees; government-appointed commissions and panels; and private review and oversight bodies. The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

[2] I also thank Nicholas M. Orlans, a biometric subject matter expert, and my RAND colleagues, John V. Parachini and Michael A. Wermuth, for their helpful comments on earlier drafts of this testimony.

because, among other things, they help authorities answer the critical question, "Who is this person?" For instance, by comparing biometric data collected from a person to other biometric records in a database, we can conduct what is called a "one-to-many" search, thus matching and linking that person to, for example, previously used identities or activities. In this context, three U.S. Government databases, all based on the biometric modality of fingerprint for automated searching, help make these matches and links possible. These are:

- The Federal Bureau of Investigation's Integrated Automated Fingerprint Identification System (FBI IAFIS), operational since 1999, which contains the ten-rolled fingerprints (*i.e.,* each digit taken "nail-to-nail") and facial photographs of approximately 52 million persons arrested in the U.S., as well as the fingerprints of approximately 20,000 known or suspected terrorists (KSTs);
- The Department of Homeland Security's Automated Biometric Identity System (DHS IDENT), which contains approximately 50 million fingerprints (most in a two-digit "flat" finger scan format which will transition to ten flats)[3] and facial photographs from various foreigners to include visitors to the U.S. under the US-VISIT program, recidivists, watchlisted persons, and asylum seekers; and
- The Department of Defense's Automated Biometric Identification System (DoD ABIS), operational since 2004, which, in close cooperation with the FBI, enables automated searching of ten-rolled fingerprint data and includes facial photographs taken from detainees and other persons of interest in places like Iraq.

The U.S. Government's use of biometric technologies has identified individuals who pose a threat to the nation's security. Examples include:

- A fingerprint match which identified Mohamed Al Kahtani, the person whom the 9/11 Commission described as the 20th hijacker.[4]
- Fingerprint matches which have identified persons in U.S. military custody in Iraq as:

---

[3] *See, e.g.,* Remarks by Secretary of Homeland Security Michael Chertoff on September 11: Five Years Later, delivered at Georgetown University, Washington, D.C., Sept. 8, 2006, on-line at http://www.dhs.gov/dhspublic/interapp/speech/speech_0287.xml, accessed Sept. 16, 2006. In his speech, Secretary Chertoff explained the change from two to ten flats "because with 10 prints taken from all visitors to the U.S., we will be able to run everybody's fingerprints against latent fingerprints that we are collecting all over the world -- in terrorist safe houses, off of bomb fragments the terrorists build, or at battlefields where terrorists wage war."

[4] *The 9/11 Commission Report, The Final Report of the National Commission on Terrorist Attacks upon the United States* (Washington, DC: U.S. Government Printing Office, 2004), 11, on-line at http://www.9-11commission.gov/report/911Report.pdf, accessed Sept. 16, 2006. For an in-depth description of the Al Kahtani match, *see* John D. Woodward, Jr., "Using Biometrics to Achieve Identity Dominance in the Global War on Terrorism," *Military Review*, Sept./Oct. 2005: 30-34, on-line as part of the *RAND Reprint* series at http://www.rand.org/pubs/reprints/RP1194/, accessed Sept. 16, 2006.

    - Persons who, because of their prior activities, pose significant threats to the well-being of U.S. forces;
    - Persons with prior U.S. criminal records;
    - Criminals wanted in the U.S.;
    - Recidivists (who had previously been in U.S. military custody, often using a different name); and
    - Persons of interest for other reasons.
- Fingerprint and face matches which have identified persons attempting to enter the U.S. as a security concern.[5]

All of these biometric matches provided helpful information, and in some cases, valuable intelligence to U.S. authorities. Many of these matches, including Al Kahtani's, occurred because of extensive DoD, FBI, and DHS cooperation. A small but significant number of these matches no doubt saved American lives.

Better Use

The U.S. Government has made progress with respect to effective use of biometrics; however, more can and should be done. Specifically, I call the Subcommittee's attention to two key areas where the U.S. Government must improve: identity management practice and the information sharing environment (ISE).

Identity management practice applies to any number of homeland security applications; for example, the foreigner seeking a U.S. visa, the registered traveler seeking to confirm her bona fides for travel, or the U.S. government employee, contractor, or military member needing a common identity credential. In general, identity management practice should focus on helping a person establish her identity, through a process that would include robust biometric vetting (*i.e.,* the one-to-many search against relevant databases), and then helping her to verify that identity, through what would include biometric verification (*i.e.,* the one-to-one comparison) to facilitate the various daily transactions that require identity management.

---

[5] "[F]rom its inception [January 5, 2004] through January 5, 2006 . . . the use of biometrics alone has allowed DHS to intercept more than 1,011 known criminals and immigration law violators—including individuals wanted for murder, rape, drug trafficking, and pedophilia." *See* Testimony of Jim Williams, Director, US-VISIT Program, Department of Homeland Security, before the Senate Appropriations Subcommittee on Homeland Security, Jan. 25, 2006, 2, on-line at http://appropriations.senate.gov/hearmarkups/JWTestimonyFINAL.pdf#search=%22jim%20williams%20us-visit%20senate%20appropriations%22, accessed Sept. 16, 2006.

We should achieve this focus, in part, by fully leveraging existing biometric databases. We should also use biometrics to "fix" or "freeze" a person's identity to defeat the use of alias identities. For example, in the case of a foreigner seeking a U.S. visa, the visa seeker's biometric data can be searched against the FBI IAFIS, DHS IDENT and DoD ABIS databases for any matches, as well as a database of all visa applicants to ensure that that individual has not previously applied under a different identity.

By complementing the identity process with a biometric, we make it easier, or more identity user-friendly, for the person—particularly when names get confused, mis-spelled, or mis-reported on watchlists of various sorts. The impartiality of biometric technologies also offers a significant benefit for society. While humans, for example, are very adept at recognizing facial features, we also have prejudices and preconceptions. The controversy surrounding racial profiling is a leading example.

Biometric systems do not focus on a person's skin color, hairstyle, or manner of dress, and they do not rely on racial, ethnic, or religious stereotypes. On the contrary, a typical system uses objective measures to recognize a specific individual. By using biometrics, human recognition can be freed from many human flaws. In essence we are enabling a person to use another convenient, impartial, reliable way to establish and verify who she is, and to make it more difficult for someone else to use her identity.

The information sharing environment (ISE) still remains polluted with stovepipes, cultural resistance, bureaucratic inertia, absence of comprehensive policy, and other impediments. Specific examples requiring immediate U.S. Government attention include:

- **Establishing a U.S. Government biometrics-based watchlist of homeland security threats.**
- **Sharing relevant biometric data with our international partners, particularly in light of global terrorism.** The U.S. Government should ask certain foreign governments to search, for example, biometric data taken from individuals in places like Iraq.
- **Creating a "net-centric" approach to the biometric-based ISE.** Too much biometric information sharing is conducted by making copies of the data and providing those copies on a physical medium, such as a compact disk, to another agency. This approach, while a temporary expedient, leads to problems with synchronization, correction, updating, and data protection. We should strive for a federated, synchronized database system based on a pooled information sharing environment managed by a community of interest.

Much of my testimony today has discussed fingerprints because that has been the biometric mainstay for our homeland security. However, the Subcommittee should note that the future will be increasingly multi-modal, featuring and fusing multiple biometric types such as fingerprint, iris, facial recognition, voice, and others. The U.S. Government's identity management practices and the ISE must be able to respond nimbly to these technological opportunities.

Summary

U.S. Government use of biometric technologies is a success story, as measured by threats identified, intelligence gained, and lives saved. Hopefully, I have provided the Subcommittee with suggestions you may find worth pursuing. I believe we are still in the very early stages of using biometric technologies for homeland security, with much more to do. As experience shows, the U.S. Government can use this significant tool for protecting the nation while preserving civil liberties. Thank you for having me testify today. I am happy to answer any questions.