NATIONAL DEFENSE RESEARCH INSTITUTE

THE ARTS
CHILD POLICY
CIVIL JUSTICE
EDUCATION
ENERGY AND ENVIRONMENT
HEALTH AND HEALTH CARE
INTERNATIONAL AFFAIRS
NATIONAL SECURITY
POPULATION AND AGING
PUBLIC SAFETY
SCIENCE AND TECHNOLOGY
SUBSTANCE ABUSE
TERRORISM AND HOMELAND SECURITY
TRANSPORTATION AND INFRASTRUCTURE
WORKFORCE AND WORKPLACE

This PDF document was made available from www.rand.org as a public service of the RAND Corporation.

Jump down to document

The RAND Corporation is a nonprofit institution that helps improve policy and decisionmaking through research and analysis.

Support RAND

Browse Books & Publications

Make a charitable contribution

For More Information

Visit RAND at www.rand.org

Explore the RAND National Defense Research Institute

View document details

Limited Electronic Distribution Rights

This document and trademark(s) contained herein are protected by law as indicated in a notice appearing later in this work. This electronic representation of RAND intellectual property is provided for non-commercial use only. Unauthorized posting of RAND PDFs to a non-RAND Web site is prohibited. RAND PDFs are protected under copyright law. Permission is required from RAND to reproduce, or reuse in another form, any of our research documents for commercial use. For information on reprint and linking permissions, please see RAND Permissions.

This product is part of the RAND Corporation occasional paper series. RAND occasional papers may include an informed perspective on a timely policy issue, a discussion of new research methodologies, essays, a paper presented at a conference, a conference summary, or a summary of work in progress. All RAND occasional papers undergo rigorous peer review to ensure that they meet high standards for research quality and objectivity.

OCCASIONAL
PAPER

DNA as Part of Identity Management for the Department of Defense

Douglas Shontz

NATIONAL DEFENSE RESEARCH INSTITUTE

This paper results from the RAND Corporation's continuing program of self-initiated research. Support for such research is provided, in part, by donors and by the independent research and development provisions of RAND's contracts for the operation of its U.S. Department of Defense federally funded research and development centers.

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.

RAND® is a registered trademark.

© Copyright 2010 RAND Corporation

Permission is given to duplicate this document for personal use only, as long as it is unaltered and complete. Copies may not be duplicated for commercial purposes. Unauthorized posting of RAND documents to a non-RAND website is prohibited. RAND documents are protected under copyright law. For information on reprint and linking permissions, please visit the RAND permissions page (http://www.rand.org/publications/permissions.html).

Published 2010 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 15213-2665
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

Preface

DNA has characteristics that some believe make it a good candidate as a biometric for either identification of individuals or verification of their identities. This paper examines this issue from several perspectives, including the technical requirements for and the policy and legal ramifications of using DNA as a biometric. This study is not exhaustive but rather is an exploratory effort designed to highlight the significant issues and potential useful applications of DNA as a biometric to assist the Department of Defense in making an informed decision about how and whether to pursue this application.

This paper results from the RAND Corporation's continuing program of self-initiated research. Support for such research is provided, in part, by donors and by the independent research and development provisions of RAND's contracts for the operation of its U.S. Department of Defense federally funded research and development centers.

This research was conducted within the Intelligence Policy Center of the RAND National Defense Research Institute, a federally funded research and development center sponsored by the Office of the Secretary of Defense, the Joint Staff, the Unified Combatant Commands, the Navy, the Marine Corps, the defense agencies, and the defense Intelligence Community. For more information on RAND's Intelligence Policy Center, contact the Director, John Parachini. He can be reached by email at johnvp@rand.org, by phone at 703-413-1100, extension 5579; or by mail at the RAND Corporation, 1200 South Hayes Street, Arlington, VA 22202-5050. More information about RAND is available at www.rand.org.

Contents

Preface iii
Summary vii
Acknowledgements ix
Abbreviations xi

DNA as Part of Identity Management for the Department of Defense 1
Introduction 1
Definition of *Biometrics* 2
Verification Versus Identification 3
DNA Technology Summary 3
Issues with and Potential Applications of DNA as a Biometric 6
Legal and Policy Issues of Overseas DNA Collection for Identification 6
Technical Issues of Overseas DNA Collection for Identification 8
Potential Applications for DNA Collection for Identification 9
Legal and Policy Issues of Domestic DNA Collection for Verification 10
Technical Issues of Domestic DNA Collection for Verification 11
Issues Beyond Privacy 12
Conclusions 13

References 15

Summary

The Department of Defense (DoD) must keep track of a large and ever-growing number of people, both known and unknown, as it executes its mission. The field associated with this responsibility is called identity management. One tool for identity management is biometrics, and, increasingly, some view DNA as a strong candidate for the expansion in biometrics because of its unique and unalterable character. However, serious questions remain about whether DNA is a viable biometric option, and it presents especially challenging questions.

This exploratory study is intended to illuminate significant issues and potential applications to assist DoD in making informed decisions about research in identity management. This paper assesses some of the issues presented by DNA data collection, storage, and use, and discusses the potential applications and implications.

This analysis led to the following key findings:

- Investment in DNA for some identification applications appears worthwhile.
- Investment in DNA for verification does not appear worthwhile.
- No studies demonstrating the value of DNA as a biometric appear to exist.
- Risk management needs can likely be satisfied with less intrusive measures than DNA.
- Collection of DNA and storage of DNA information within DoD requires a systematic approach that includes identifying priorities and risks.
- Little or no reliable cost data exist.

DoD should therefore begin a systematic effort to evaluate the viability of DNA in identity management. The DoD needs to systematically

- evaluate and state its priorities for identity management
- evaluate and state the risks identity management is intended to address
- explain how using biometrics reduces those risks
- identify risks or priorities that can only be addressed by DNA
- analyze the costs and benefits of expanding the use of DNA in identity management
- develop policies regarding collection, analysis, use, and storage of DNA information.

At this time, DNA as a biometric appears a worthwhile investment for narrow, targeted applications. Less complicated and more robust technologies, such as fingerprint and iris scans, should be favored for broad-based biometric applications.

Acknowledgements

The author would like to thank Keith Gierlack for his hard work in contributing to the research for the study and Jerry Sollinger for his valuable insights to improve this paper.

Abbreviations

AFRSSIR	Armed Forces Repository of Specimen Samples for the Identification of Remains
CAC	Common Access Card
CODIS	Combined DNA Index System
DNA	deoxyribonucleic acid
DoD	U.S. Department of Defense
FRV	Forensic Response Vehicle
IED	improvised explosive device
PCR	polymerase chain reaction
PIN	Personal Identification Number
SOFA	Status of Forces Agreement
STR	short tandem repeat

DNA as Part of Identity Management for the Department of Defense

Introduction

The Department of Defense (DoD) has a growing need to improve its capabilities in the field of identity management, which involves a full spectrum of administrative functions and challenges to identify people and maintain records about them. As stated in a 2007 Defense Science Board report,

> In any very small group there is no need for identity management. However, whenever populations become more numerous, especially if they are not always or ever in physical contact with each other, distinguishing among individuals becomes steadily more important. In national security matters, as friend/foe distinctions such as clothing (uniforms) diminish in incidence and usefulness, this point is underlined.[1]

The goal, then, of identity management is to reduce the risk that a person is incorrectly denied access, is incorrectly granted access, or is not detained, depending on the particular objective. In other words, DoD must keep track of a large and ever-growing number of people, both known and unknown, as it executes its mission. One tool for identity management is biometrics, and DoD is one of many government agencies expanding or considering expanding use of biometrics for both DoD personnel ("blue" personnel) and people being sought by DoD ("red" personnel). However, using biometrics for identifying blue and red personnel both inside and outside the United States poses important legal, policy, and cost/benefit questions.

Increasingly, some view DNA as a strong candidate for the expansion in biometrics because of its unique and unalterable character, i.e., everyone's DNA is different and it cannot be changed. However, serious questions remain about whether DNA is a viable biometric option for identity management applications, and it presents especially challenging questions about appropriate collection, use, and investment decisions. For example, are there privacy restrictions or concerns associated with using DNA for identification and tracking? Will research in DNA as part of identity management technology provide greater benefits than other avenues of research, such as iris scan or facial recognition technologies?

This exploratory study is intended to illuminate significant issues and potential applications to assist DoD in making informed decisions about pursuing various paths of research in biometrics and the broader field of identity management. This study is not intended to be a comprehensive analysis of DNA in the realm of biometrics. Rather, the goal is to place the

[1] U.S. Department of Defense, Defense Science Board, 2007.

above questions in the context of uses and intended outcomes—especially in the realm of mass collection. In this paper, I assess some of the issues presented by DNA data collection, storage, and use, and discuss the potential applications and implications of expanded use, including potential legal, policy, and technical limitations. The analytical results can help DoD to effectively plan for future investments in, and uses of, biometrics.

In the sections that follow, I briefly define DNA within biometrics, summarize DNA technology, and explain the important difference between *identification* and *verification* within the identity management field. I then analyze key issues raised by potential expansions of DNA use and explore candidate applications for DNA as a biometric. This analysis leads to the following key findings:

- Investment in DNA for some identification (red force) applications appears worthwhile.
- Investment in DNA for verification (blue force) does not appear worthwhile.
- No studies demonstrating the value of DNA as a biometric for identification or verification, either in general or as compared with other biometric modalities, appear to exist.
- Risk management needs can likely be satisfied with less intrusive measures than DNA.
- Collection of DNA and storage of DNA information within DoD requires a systematic approach that includes identifying priorities and risks.
- Little or no reliable cost data exist.

Definition of *Biometrics*

Biometrics is defined as "the measurement and analysis of unique physical or behavioral characteristics ([such] as fingerprint or voice patterns) especially as a means of verifying personal identity."[2] The DoD Biometric Task Force defines *biometrics* as "measurable, physiological, and/or behavioral characteristics (fingerprints, iris, DNA, voice, facial features, etc.) that are distinct and can be used to verify the identity of an individual."[3]

In this sense, DNA does not exactly fit the definition of a biometric. DNA could arguably be described as a physiological characteristic, but as a biometric, it requires more measurement and analysis than do other biometrics. To use DNA, a physical sample must initially be collected and stored, and then, at the time needed, another physical sample must be collected and analyzed, with the results compared against the first sample. In contrast, the typical biometric uses a template or other easily and automatically extracted representation in some mathematical "space." For example, for fingerprints and facial recognition, an initial image or impression is collected and compared against another image later. This difference is a fundamental one of some import, as will be explained in the rest of the paper.

Other key differences, as stated by the International Biometrics Group, include the fact that "DNA matching is not done in real-time, and currently not all stages of comparison are automated. [Also,] DNA matching does not employ templates or feature extraction, but rather represents the comparison of actual samples."[4] In other words, DNA requires laboratory pro-

---

2 *Merriam-Webster's Collegiate Dictionary*, 2003.

3 U.S. Department of Defense, 2008.

4 International Biometrics Group, 2010.

cessing and "template" extraction that is neither automated nor currently rapid. Further, the Defense Science Board noted that there is "definitional debate within the U.S. government regarding the proper 'status' of DNA as a 'true biometric,'" so the Defense Science Board task force defined DNA as a "'biometric modality,' even while recognizing its unique character."[5]

For purposes of this paper, I consider DNA a biometric, but it is important to understand that it differs fundamentally from other biometrics. DNA can reveal facts beyond simple identity of an individual, and new types of information are constantly being discovered in DNA. In fact, the issue was considered serious enough that Congress passed the Genetic Information Nondiscrimination Act of 2008 (P.L. 110-233), which bars health insurers from denying coverage and employers from making hiring decisions based on whether a person's DNA indicates the potential for developing a disease in the future.

Verification Versus Identification

Biometrics have two basic uses: identification and verification. Identification is sometimes referred to as "one-to-many" matching. The best-known use of biometric identification is in criminal forensics and can work two ways. First, for example, the police may collect a fingerprint at a crime scene and "run" the print against a database of previously collected prints to look for a possible match. Second, the police may arrest someone and run his or her fingerprints against a database of unidentified prints collected from past crime scenes, again seeking a possible match. In each case, the goal is to identify one unknown person or piece of information by comparison with many known items.

Verification, on the other hand, is referred to as "one-to-one" matching and is commonly applied for access control. For example, when logging into a DoD computer, a user must insert his or her Common Access Card (CAC) into the reader and then enter a Personal Identification Number (PIN). The system matches the CAC and PIN to the entry for that individual user in the database of authorized users. This verifies that the person sitting at the computer is who he or she claims to be and is authorized to have access. Biometrics are increasingly being applied in a similar fashion, most frequently with fingerprint verification.

DNA Technology Summary

The state of DNA biometric technology can be summed up as expensive and slow, but accurate for exact matches. The process of analyzing a DNA sample and obtaining a profile consists of four steps: collection, extraction, amplification, and sequencing. First, the biological sample is carefully collected to limit the possibility of contamination. Once the biological sample has been collected, it must be handled and stored in, at a minimum, stable environmental conditions to prevent degradation from excessive heat or ultraviolet radiation exposure, such as from sunlight. The biological sample must also be stored in a nonplastic container, because condensation within a plastic container could cause contamination.[6]

---

5 U.S. Department of Defense, Defense Science Board, 2007.

6 U.S. Department of Justice, National Institute of Justice, 2002, p. 14.

Second, during extraction, the DNA is removed from the nuclei of the sample if the cells are from blood or other bodily fluids, or from the mitochondria if the sample is from hair, teeth, or bone. Mitochondrial DNA is less preferable for creating a profile because only maternal relatives have identical mitochondrial DNA.[7] Extraction involves mixing the sample with a loading dye to increase the density of the DNA. The sample is then mixed with an ionized gel to separate the DNA from the rest of the biological material.[8]

Third, the DNA is amplified, or copied, millions of times to obtain enough DNA to analyze. This is accomplished through a technique known as polymerase chain reaction (PCR). Since PCR copies the sample DNA millions of times, only a very small amount of biological material is needed for analysis.[9] This is in contrast to early DNA processing that required large amounts of biological material, which were not always available at a crime scene and increased the risk of contamination.

Finally, the DNA is sequenced to obtain the unique nucleic acid base pairing. This part of the process can be conducted with any number of commercially available automated genetic analyzers. Once this is accomplished, individual regions of the DNA strand can be examined. DNA is made up of four nucleotides: adenine, thymine, cytosine, and guanine. Since DNA is double-stranded, the strands are complementary, so that the same nucleotides always match up the same way to form the "base pairing," i.e., adenine with thymine and cytosine with guanine. The analysis looks for repeated sequences of base pairs, referred to as short tandem repeat (STR) analysis.[10]

Different people have different numbers of repeats at STR locations on the DNA strand. Since approximately 99.7 percent of human DNA is common, the remaining 0.3 percent contains the unique sequences needed to create a DNA profile,[11] and STRs are used to identify these unique sequences.

The more STR locations examined, the less likely two people would share the same profile. Currently the FBI uses 13 STR regions[12]—or loci—to create a DNA profile,[13] also known as a "DNA fingerprint." This allows for a very low statistical possibility of two people having identical repeat patterns at the examined locations.[14]

---

7 U.S. Department of Justice, National Institute of Justice, 2002, p. 7.

8 University of Arizona, 2002.

9 U.S. Department of Justice, DNA Initiative, "Steps in DNA Sample Processing," no date.

10 University of Michigan, no date.

11 Soltysiak and Valizadegan, no date.

12 According to the U.S. Department of Justice DNA Initiative, "[t]he Federal Bureau of Investigation (FBI) has chosen 13 specific STR loci to serve as the standard for CODIS. The purpose of establishing a core set of STR loci is to ensure that all forensic laboratories can establish uniform DNA databases and, more importantly, share valuable forensic information" (U.S. Department of Justice, DNA Initiative, "STR Analysis," no date). By comparison, the United Kingdom uses 10 loci (National Institute of Standards and Technology, no date).

13 U.S. Department of Justice, National Institute of Justice, 2002, p. 6.

14 According to the U.S. Department of Justice DNA Initiative "the likelihood that any two individuals (except identical twins) will have the same 13-loci DNA profile can be as high as 1 in 1 billion or greater" (U.S. Department of Justice, DNA Initiative, "STR Analysis," no date). As an example, a New York State Police Crime Laboratory analyst found an exact match between DNA from two different left arms recovered from the World Trade Center. Further investigation revealed that the arms were from a pair of identical twin brothers who were both killed on September 11, 2001.

Once the profile has been created, it can be interpreted manually by visually comparing the STR locations examined, or it can be entered into a database so that computer analysis can compare the profile against previously stored profiles. This process can take four to five hours,[15] not including transportation and preparation time. New technologies promise significant reductions in the processing time, thus allowing much faster analysis of collected biological samples. An example is the Forensic Response Vehicle (FRV) in the United Kingdom. The FRV is a mobile laboratory that processes and analyzes DNA samples at a crime scene and enters them into a database to search for a match, eliminating the time required to transport samples to a central laboratory.[16]

DNA testing can result in three types of results: inclusive, exclusive, or inconclusive. When DNA profiles match, the individual is "included" as a potential source. The strength of inclusion depends on the number of STR locations examined. As previously stated, the more locations examined during the test, the higher the probability of a confirmed match. An "included" result does not necessarily mean the two DNA profiles are exact, just that there is a high degree of similarity. Since relatives have similar DNA, at times it is necessary to examine the two profiles manually to exclude other family members. If the DNA profile does not match, then the individual is excluded as a potential source.[17] An inconclusive result can be caused by contamination of the biological sample or a lack of sufficient quantity of biological material for testing.[18]

The largest DNA profile database in the United States is the Combined DNA Index System, or CODIS, administered by the FBI. As noted above, FBI scientists analyze 13 loci when creating a DNA profile. This profile is stored in CODIS, and the computer automatically scans other profiles for possible matches. The CODIS database contains DNA profiles from convicted violent criminals and samples taken from crime scenes. All 50 states and the FBI and U.S. Army participate in this program, which allows DNA profiles to be shared by law enforcement agencies across the country.[19]

Importantly, for consideration of expanding DNA use, recent anecdotes have pointed to a potentially serious problem with false positives for partial matches using the FBI's standard of 13 loci matching. Many apparently improbable matches were found in a state criminal DNA database, well in excess of what the FBI's statistics predicted should be found. The profiles in question matched at 9 of 13 loci, which the FBI predicts has only a "1 in 113 billion" chance of happening for two unrelated people.[20] While the analysis did not show an exact profile match, it did raise the potential for a large number of false positives and undermined the assertions of DNA profile reliability.

---

15 European Commission, 2005, p. 64.

16 Kemp and Pinchin, 2007.

17 U.S. Department of Justice, National Institute of Justice, 2001, p. 4.

18 U.S. Department of Justice, National Institute of Justice, 2001, p. 5.

19 Jones, 2006.

20 Felch and Dolan, 2008.

Issues with and Potential Applications of DNA as a Biometric

Important issues arise at all points of the process of using DNA as a biometric. The most important of these are

- legal and policy issues of collection, storage, and disposition
- technical challenges of collection and analysis, especially for mass collection.

There is also the overarching issue of whether expanding DNA applications is an efficient use of limited resources, i.e., whether the costs of using DNA outweigh the benefits and whether other biometric modalities offer better opportunities to manage identities. Analysis of all these issues depends on the particular application of DNA technology. Unfortunately, the common thread through these issues and potential applications is that a systematic and rigorous cost-benefit analysis has not been done, and, in fact, little cost data of any kind are available. Thus, this analysis is a qualitative one that aims at highlighting important considerations.

The sections that follow seek to analyze the legal, policy, and technical issues regarding use of DNA as a biometric in two areas: overseas use for identification and domestic use for verification.

Legal and Policy Issues of Overseas DNA Collection for Identification

Most of DoD's mission is focused outside the United States, so the department needs to consider the implications of collecting and analyzing DNA in combat zones for purposes of identification, especially mass collection. In general, few legal impediments stand in the way of DoD's use of DNA for identification in overseas military operations, but DoD still needs to be prepared to deal with these legal issues before collecting a person's DNA. To think about these issues, it may be useful to separate the overseas world into at least two categories—combat zones and other areas.

In places such as Iraq and Afghanistan, there are relatively few concerns about legal barriers. For example, until the 2008 Status of Forces Agreement (SOFA) and Strategic Framework Agreement were signed with the Government of Iraq, the U.S. military was effectively unconstrained if it decided to collect DNA from every non-U.S. person detained or entering a U.S. facility. Under the SOFA, the United States must "respect Iraqi laws, customs, traditions, and conventions and . . . refrain from any activities that are inconsistent with the letter and spirit of this Agreement."[21] However, it is likely that the Unites States would be allowed to collect DNA from any Iraqi detained during military operations.

Legal barriers would also be low for covert DNA collection in noncombat countries, similar to those for other intelligence collection operations, while restrictions would likely be higher in Australia, Canada, New Zealand, and the United Kingdom, where the U.S. has agreements about limits on intelligence collection.

By comparison, in the United States, several states routinely compare the DNA of violent offenders against databases of unidentified samples collected from crime scenes. In fact, the Department of Justice announced plans to exercise previously granted authority to collect

[21] Agreement Between the United States of America and the Republic of Iraq on the Withdrawal of United States Forces from Iraq and the Organization of Their Activities During Their Temporary Presence in Iraq, 2008.

DNA samples from anyone arrested by a federal law enforcement agency,[22] and several states already have some similar form of legislation in effect.[23] So far, no one has successfully challenged a state law requiring collection of DNA.

From a policy perspective, the biggest question with DNA collected outside the United States is whether there is sufficient value derived from the activity, i.e., whether the benefits derived outweigh the investment compared with other areas where resources could be applied. For example, would money spent on DNA biometric technology have been better spent on improving fingerprint technology or on detecting and defeating improvised explosive devices (IEDs)? RAND researchers were unable to find any studies of foreign DNA collection and analysis examining whether mass collection of DNA had provided greater benefits to the United States than other efforts could have produced—a finding confirmed by a member of the National Science and Technology Council's Subcommittee on Biometrics and Identity Management in late 2008. While there are studies of DNA analysis technology (examining error rates, repeatability, etc.), a true cost-benefit analysis is important for policymakers to be able to make informed decisions. There may be anecdotes about identification of a wanted individual from a DNA database, but this does not necessarily mean the capability merits the same level of or additional resources when compared with other DoD investments. A serious analysis of DNA's value as a biometric should be conducted before engaging in further mass collection of DNA from detainees or other foreign personnel.

For example, news reports in 2008 indicated DoD had collected DNA from more than 80,000 people, mostly in Iraq and Afghanistan,[24] and created a database of profiles. This database is likely part of or related to the Joint Federal Agencies Intelligence DNA Database referenced by a March 2007 Defense Science Board report as containing "15,000 DNA profiles"[25] and referenced by at least one news report.[26]

Further, policies need to be developed to guide the military. For example, what should the United States do with the DNA data from Iraqi, Afghan, and other detainees? How long should the United States maintain this information? Should the United States allow Iraqi or Afghan authorities to have access? Or a copy? Would this create a target list for people engaged in ethnic or tribal conflict?[27] As the U.S. military engagements in Iraq and Afghanistan continue, questions like these must be addressed to develop clear policies and ensure that collection, storage, dissemination, or destruction of DNA information does not harm innocent people or result in the loss of useful information.

In other words, if DoD decides to pursue a robust capability to engage in broad collection of DNA to generate a profile database, the department must address several key points, including the following:

- which people should be targeted for collection

---

22 "DNA-Sample Collection and Biological Evidence Preservation in the Federal Jurisdiction, Final Rule," 2008.

23 Nakashima and Hsu, 2008.

24 As of December 2008, the Joint Federal Agencies Intelligence DNA Database has more then 80,000 profiles, an increase of more than 400 percent from 2006. See Eisler (2008).

25 U.S. Department of Defense, Defense Science Board, 2007.

26 "U.S. Secretly Collecting Detainee DNA," 2008.

27 Schachtman, 2007.

- where the capability will be housed (i.e., who "owns" the DNA database?)
- implementation procedures in the field
- policies for storage, protection, dissemination, and disposition of the DNA information for the longer term.

Technical Issues of Overseas DNA Collection for Identification

Applying DNA as a biometric for identification presents a difficult set of technical challenges. The most likely scenario for identification with DNA involves collection of an unknown DNA sample from a site of interest or collection from a detained individual. For example, a house in Iraq where weapons are discovered may contain clothing with bloodstains. The DNA could be analyzed and compared with a database of known persons of interest. Similarly, DNA from a detained person could be run against a database of DNA from unidentified people, e.g., DNA previously found on an IED.

Under these circumstances, cost and sample contamination as well as timeliness for collecting and analyzing a sample are significant issues. First, deploying a DNA analytical capability in an environment such as Afghanistan would be more expensive than using fingerprints. Under controlled circumstances in the United States, the current cost of DNA analysis is estimated to run as low as $50 per sample[28] to as high as $500 for a forensically rigorous analysis,[29] i.e., for samples potentially part of criminal prosecutions. However, it is unclear to what extent these widely varying costs incorporate the cost of the facilities and personnel required to perform the work. Further, costs could also increase substantially when taking into consideration transportation, security, and the infrastructure associated with deploying a capability in the field. In fact, the Defense Science Board highlighted this exact issue by noting that "the field operational utility of DNA is held back by the delays inherent in the physical transport of the specimens to the lab, and the costly and lengthy processing."[30]

Even in the United States, current capacity is a limiting factor in using DNA. The FBI's budget request to fund CODIS for Fiscal Year 2008 stated that the system cannot accommodate more than 10 million profiles, while forecasting a continued increase in the number of profiles from 4 million in 2006 to 14 million in 2009.[31] Maintaining CODIS in its current form requires over $10 million per year.[32] However, CODIS costs represent only the database of DNA profiles and do not include the cost of collecting and analyzing DNA samples, which is the "bottleneck" where the backlog of samples accumulates.[33]

Managing DNA in a war zone poses additional challenges. Sample contamination during field operations would be difficult to avoid. Ideally, a detained individual would be put in an area that would afford uncontaminated sample collection, but even this is problematic. The bigger challenge is with DNA collected from open-environment sources, such as an IED site.

---

[28] See, e.g., U.S. Department of Justice, National Institute of Justice, 2007, stating that economies of scale could reduce the cost to $50 per sample analyzed.

[29] This is according to a member of the Mississippi Bureau of Investigation, Cold Case Squad (interviewed by the researchers in February 2008).

[30] U.S. Department of Defense, Defense Science Board, 2007, p. 32.

[31] U.S. Department of Justice, Federal Bureau of Investigation, 2008.

[32] U.S. Department of Justice, Federal Bureau of Investigation, 2008.

[33] Willing, 2007.

DNA degrades quickly when exposed to sunlight, humidity, and bacteria. Thus, it is important to collect samples in the open environment as quickly as possible after discovery. Also, training DoD personnel in collection procedures for both detained individuals and samples in the environment is critical to maximizing benefit but a challenge in an operational threat environment. A similar challenge was faced in using fingerprint biometrics in Iraq, though the process of collecting that information is less difficult than for DNA, and fingerprints are more stable in the open environment.

Potential Applications for DNA Collection for Identification

Given the range of issues, the most beneficial application of DNA as a biometric for DoD appears to be as an intelligence tool for identification that takes advantage of DNA's unique characteristics. In addition to the current intelligence efforts of collecting DNA from foreign detainees (see above), another potential application is familial searching. In most scenarios, the desired outcomes for analyzing DNA are exact matches. However, with familial searching, the goal is partial matching to identify possible family members of the individual being sought. The UK government has successfully used familial searching for cold case criminal investigations. In one case, the police arrested a woman for drunk driving and found a familial match with the unidentified DNA of a wanted rapist.[34] The police then questioned the woman's brother, who confessed to the rapes.

Familial searching may be especially useful in Arab cultures where family and tribal links could be used for social network analysis. Familial searching is feasible with current technology and seems most promising in terms of providing information that cannot be gathered through other means, which may make it most suitable for intelligence applications.[35] However, it may still be prohibitively expensive for broader application, and attempts to find partial matches may run into the false positive issue discussed above.

As understanding about genetic links to physical and mental health increases, DNA may also provide useful information about other foreign intelligence targets. Intelligence agencies could collect the DNA of senior foreign government and military officials through clandestine operations to obtain information about who is susceptible to certain diseases or conditions. This could be an important indicator for when future changes in senior leadership might occur. The DNA could also highlight familial links (as noted above) that could help shed light on the centers of power within foreign governments or even help identify covert intelligence operatives.

The strongest argument for having robust capabilities for identification is the fact that DNA is a latent identifier. People do not leave pictures of their faces or irises everywhere they travel, but they do leave DNA (and fingerprints). Further, direct physical contact with the targeted person is not necessary. For example, cigarette butts or drinking glasses provide opportunities to collect DNA. This aspect is critical for the likely applications and seems to support further work on DNA at some level.

The biggest obstacle would likely be the technical challenge of collecting an uncontaminated sample and transporting it for analysis. Such an approach would also take significant

---

[34] Nakashima, 2008.

[35] See Bhattacharya (2003) noting that the U.S. military probably identified Saddam Hussein by comparing a DNA sample with personal items collected from his quarters. He was also fingerprinted by the FBI.

time to begin producing useful information because of the need to have samples from many people to aid network analysis or leadership forecasting.

As with all potential expansions of DNA use, the biggest question is whether the costs would provide sufficient benefits. With limited research budgets and competition for resources, the case would have to be made that DNA information is of such high value that it should take priority over other intelligence collection efforts. Compared with other investments in DNA, this application appears to require the smallest investment in infrastructure and training to yield desired benefits because of its more narrowly targeted nature. Thus, even though it would not be likely to gain priority over improved human intelligence collection or improved sensor technology, it might be attractive in very limited applications.

Legal and Policy Issues of Domestic DNA Collection for Verification

Using DNA as a biometric for verification presents a host of issues, including privacy and technical implementation, and is not a viable application at this time.

One of the biggest concerns about using DNA for verification is the assertion that it violates people's privacy. The focus of the privacy argument is that DNA analysis could potentially reveal information about people's health. This information could then be abused and exploited, e.g., making hiring and firing decisions based on the presence of a potential health issue. If DNA were implemented for verification, one way to alleviate some concerns would be to limit the analysis to only those portions of people's DNA that can be used to verify identity and then destroy the physical samples. However, even if these measures were put in place in an effective manner, it would be difficult to assuage public concerns about privacy.

In terms of trying to implement DNA for verification, there do not appear to be any major legal obstacles to using DNA as a biometric for verification at DoD facilities. DNA would likely be treated like other personal information collected for security clearances and access control. People voluntarily participate—referred to as "enrolling"—for purposes of obtaining employment. The voluntary/consensual nature of the relationship removes most potential legal issues regarding collection and analysis of DNA samples.

Any legal challenge would likely argue that using DNA is unreasonable. Courts allow the "reasonable"[36] collection of information, applying different standards depending on the context.[37] Courts will allow information to be collected if there is a "rational basis" for doing so when it does not affect fundamental rights. A stricter "compelling need" test is applied when a person's fundamental rights will be affected. However, courts are generally willing to accept the government's assertion of what constitutes a compelling need to enhance or maintain security. Further, the government could argue that a cheek swab for a DNA test is "minimally intrusive."[38] However, someone challenging DNA use could argue that such use is unreasonable given other, less intrusive options, such as fingerprint and iris scans. To date, no such challenge has apparently been presented in court.

However, significant policy challenges would arise in trying to implement DNA as a biometric for verification. DNA is especially sensitive because of both the perceived and real threat of misuse or misappropriation. Further, unlike other forms of identity theft, once DNA infor-

[36] See, e.g., Liu, 2008.

[37] See, e.g., Woodward, 2008.

[38] See, e.g., Woodward, 2008.

mation has been stolen, it is gone, and the affected individual(s) will always be at risk. While DNA is currently collected from all active duty personnel and stored at the Armed Forces Repository of Specimen Samples for the Identification of Remains (AFRSSIR) for purposes of identification for combat deaths, DoD treats civilians differently. Civilian DoD employees who are deployed in the field submit DNA samples to the repository, but civilians working strictly domestically do not because they are not considered at significant risk of being killed in a fashion that would require DNA to identify remains. Thus it seems likely that some DoD employees and probably members of Congress would resist a proposal to use DNA more broadly to verify the identities of DoD personnel.

If permitted to use DNA for verification, DoD would have to develop procedures for protecting collected DNA information well beyond those needed to protect other personally identifiable information and biometric data. As noted earlier, DoD would have to purchase and maintain a large computer infrastructure just to store the DNA data. In addition, DoD would need to take steps to secure the DNA information to ensure that people's personal information is protected from the point of initial collection through computer storage to deletion.

Finally, DoD would have to be prepared to address destroying the DNA data for personnel who "un-enroll." Again, since civilian employees differ from active duty military, DoD could have a difficult time arguing the need to maintain someone's DNA information after he or she separates from the department. And, as is the case with protecting the information while it is being used, the information must be protected when it is destroyed.

Technical Issues of Domestic DNA Collection for Verification

Even if policy issues could be overcome, DNA is not a viable option for verification from either a technical implementation or a cost standpoint. First, as noted in the above explanation of verification, biometrics (usually fingerprints) are increasingly being used to verify the identity of authorized—or "blue force"— personnel for access control. Effective access control requires an immediate (or nearly so) response. It is not feasible to have people wait three or more hours—or even the half-hour predicted by some for the future of DNA analysis—required to verify identity using DNA while trying to enter the Pentagon or gain access to parts of the Embassy in Baghdad. At the U.S. Embassy in Baghdad, a long line of people waiting to enter a building can present a significant security risk because of the opportunity to be targeted. One need only recall the CIA employees being shot in 1993 while waiting in their cars to enter CIA grounds[39] and the attacks on personnel entering and leaving the Green Zone in Iraq.

Second, the cost of using DNA for verification at access control points would be prohibitive. As noted above, estimates of the current cost per sample range widely. Even if the cost is at the low end of current estimates, or drops further with improved technology,[40] costs would still prevent implementation for a building such as the Pentagon, for which thousands of samples would need to be run every day. For example, at $50 per sample and over 20,000 employees and contractors entering the Pentagon every day, that is an annual cost of over $250 million.

---

[39] See, e.g., Ayres, 1993.

[40] Advances in technology could reduce analysis time and cost in the future. For example, a researcher at the National Science Foundation Center for Identification Technology Research (interviewed by the author via telephone in March 2009) said that one company is developing a device that can perform DNA amplification in the analysis process in 20 to 30 minutes, using advances in microfluidics and the "lab on a chip" concept. However, the technology is not yet proven to be forensically rigorous and reliable and at this point would be significantly more expensive than current technology.

A potential alternative would be to use DNA for limited purposes of random screening or like "secondary inspection" at a border. However, given the biometric technology capabilities for fingerprints and iris scans, DNA still appears cost-prohibitive because of its collection and analysis process.

Further, the cost of storing, maintaining, and protecting the DNA information would be high. A database of every DoD employee's DNA profile would be a huge amount of information, plus the associated infrastructure to collect and analyze the physical samples.[41] To be useful for verification, the information in the computer database would have to be backed up and constantly checked for quality assurance purposes to ensure that the data are not corrupted. This would require a major investment by DoD that would far outweigh any benefit in terms of reducing risk of unauthorized access to DoD facilities. Unfortunately, no information about the cost of maintaining such a system could be obtained beyond the annual operating cost of CODIS.

Issues Beyond Privacy

The issue of privacy and DNA collection (as well as all biometric use) has been discussed extensively in legal, trade, and news publications. As noted above, the major focus of privacy concerns falls on the potential information that could be revealed from DNA analysis in the future, such as diseases carried by the individual. Privacy concerns for all biometrics are still being examined in attempts to balance the needs of national security (e.g., Iraq) and domestic security (e.g., law enforcement), and DNA requires special attention because of its qualitative difference from other biometrics in terms of the information it contains.

Nevertheless, there are significant additional concerns, beyond privacy of the individual, that affect analysis of this matter. First, extensive policies, procedures, and training would have to be developed before implementing any sort of robust capability with DNA for any application. In fact, the Defense Science Board's report on biometrics concluded that "policy, technical, and organizational efforts are still required,"[42] and DoD personnel have publicly acknowledged that technology has been deployed ahead of policy.[43] These concerns cover all biometrics, and DNA seems to be inherently more complex than most because of its sensitivity and the technical requirements for collection and analysis.

Second, there are the ever-present insider and outsider threats associated with collecting sensitive personal information. A database of DNA profiles—and likely other identifying information—for thousands of foreign and possibly U.S. personnel would be a target of significant interest for foreign intelligence services. A trusted insider could compromise the data, and foreign intelligence agencies constantly look for vulnerabilities in U.S. computer networks, which would be an important component of any DNA identity management system.

---

[41] This does not include the large cost if physical samples were maintained, like the samples of all active duty personnel at the AFRSSIR.

[42] U.S. Department of Defense, Defense Science Board, 2007.

[43] Magnuson, 2007.

Conclusions

The goal of using biometrics is risk management, i.e., to reduce the risk of making a mistake regarding someone's identity (in both the identification and verification arena). As stated by the National Science and Technology Council Subcommittee on Biometrics, "The primary goal of the [Identity Management] process is to assign attributes to a digital identity and to connect that identity to an individual."[44] In other words, organizations try to determine a person's identity based on digitally stored information.

DNA as a biometric presents some intriguing potential for DoD in limited applications of identification for intelligence purposes. DNA collection for broad-based identification through mass collection has not been shown to be sufficiently useful, and using DNA for verification is not an option at this time (and may very well never be given the privacy and other concerns). Also, little to no information is available that shows the costs and benefits of using DNA or that could be used to compare DNA with other biometric modalities. In other words, there is no evidence that investment of limited resources should be targeted to DNA rather than other research areas. By contrast, some examples of successful and important identifications have been made using fingerprints.[45] This raises the question of whether the money and time spent to collect and analyze over 80,000 DNA samples of Iraqi and Afghan detainees could have been put to better use. Finally, important questions remain about DNA's reliability for partial matching. Thus, selective use of DNA technology for intelligence purposes appears to be more promising.

Further, no apparent effort has been undertaken to organize research of DNA technology and applications or to prepare policies for dealing with the large amounts of DNA information already collected and that could be collected in the future. However, arguments about a perceived need to use DNA are diminished as other biometric technologies (fingerprint, iris scan, etc.) improve. Too often, technology gets ahead of policy and is fielded without policies, organizational support, and necessary infrastructure. It is likely that DNA collection and analysis in Iraq and Afghanistan started without an analysis of the goals, objectives, costs, and benefits, especially compared with other possible expenditures. Therefore, DoD should begin such a systematic effort immediately, because significant resources would be required to develop a robust DNA biometric capability. DoD needs to systematically

- evaluate and state its priorities for identity management
- evaluate and state the risks identity management is intended to address
- explain how using biometrics reduces those risks
- identify risks or priorities that can only be addressed by DNA
- analyze the costs and benefits of expanding the use of DNA in identity management
- develop policies regarding collection, analysis, use, and storage of DNA information.

The field of identity management will continue to grow along with the scope of DoD operations. DoD will want to use its limited resources in a manner that provides the greatest benefits for the most compelling needs. Biometrics will continue to be a part of this, and an organized approach to policy development and technology research is critical. At this time,

[44] National Science and Technology Council Subcommittee on Biometrics and Identity Management, 2008.

[45] See, e.g., Shannon, 2006.

DNA as a biometric appears a worthwhile investment for narrow, targeted applications. Less complicated and more robust technologies, such as fingerprint and iris scans, should be favored for broad-based biometric applications.

References

Agreement Between the United States of America and the Republic of Iraq on the Withdrawal of United States Forces from Iraq and the Organization of Their Activities During Their Temporary Presence in Iraq, November 2008.

Ayres, B. Drummond, Jr., "Gunman Kills 2 Near C.I.A. Entrance," *The New York Times*, January 26, 1993.

Bhattacharya, Shaoni, "Fast-Track DNA Tests Confirm Saddam's Identity," *New Scientist*, December 15, 2003.

"DNA-Sample Collection and Biological Evidence Preservation in the Federal Jurisdiction, Final Rule," *Federal Register*, Vol. 73, No. 238, December 10, 2008, pp. 74932–74943.

Eisler, Peter, "Pentagon Keeps DNA Files on 80K Detainees, Terror Suspects," *USA Today*, December 11, 2008.

European Commission, Joint Research Centre, Institute for Prospective Technological Studies, *Biometrics at the Frontiers: Assessing the Impact on Society*, March 2005. As of March 19, 2010: http://ipts.jrc.ec.europa.eu/publications/pub.cfm?id=1235

Felch, Jason, and Maura Dolan, "FBI Resists Scrutiny of 'Matches,'" *Los Angeles Times*, July 20, 2008.

International Biometrics Group, "Is DNA a Biometric?" As of March 10, 2010: http://www.biometricgroup.com/reports/public/reports/dna.html

Jones, Phillip, "Using Biometric Technology to Advance Law Enforcement," *Forensic Magazine*, August/September 2006. As of March 19, 2010: http://www.forensicmag.com/articles.asp?pid=104

Kemp, Steve, and Richard Pinchin, "Decreasing Turnaround Time of DNA Analysis by Improving Processes in the Laboratory," *American Laboratory*, September 2007. As of March 19, 2010: http://www.statewatch.org/news/2005/mar/Report-IPTS-Biometrics-for-LIBE.pdf

Liu, Yue, "Identifying Legal Concerns in the Biometric Context," *Journal of International Commercial Law and Technology*, Vol. 3, No. 1, 2008.

Magnuson, Stew, "Military Identity Technology Leaps Ahead of Policies," *National Defense Magazine*, November 2007.

Merriam-Webster's Collegiate Dictionary, Eleventh Edition, 2003.

Nakashima, Ellen, "From DNA of Family, a Tool to Make Arrests," *The Washington Post*, April 21, 2008.

Nakashima, Ellen, and Spencer Hsu, "U.S. to Expand Collection of Crime Suspects' DNA," *The Washington Post*, April 17, 2008.

National Institute of Standards and Technology, Chemical Science and Technology Laboratory, "Core STR Loci Used in Human Identity Testing," no date. As of March 19, 2010: http://www.cstl.nist.gov/biotech/strbase/coreSTRs.htm

National Science and Technology Council Subcommittee on Biometrics and Identity Management, *Identity Management Task Force Report*, 2008.

Public Law 110-233, Genetic Information Nondiscrimination Act of 2008, May 21, 2008.

Schachtman, Noah, "Iraq's Biometric Database Could Become 'Hit List': Army," *Wired.com*, August 15, 2007. As of March 19, 2010:
http://blog.wired.com/defense/2007/08/also-two-thirds.html

Shannon, Paul, "Fingerprints and the War on Terror," *Joint Forces Quarterly*, No. 43, 4th quarter, 2006.

Soltysiak, Shannon, and Hamed Valizadegan, *DNA as a Biometric Identifier*, Michigan State University, no date. As of March 19, 2010:
http://www.cse.msu.edu/~cse891/Sect601/CaseStudy/DNABiometricIdentifier.pdf

University of Arizona, General Biology Program for Teachers, "Using Genetic Evidence to Evaluate Group Behavior," 2002. As of March 19, 2010:
http://biology.arizona.edu/sciconn/lessons2/Vuturo/vuturo/gel.htm

University of Michigan, Pollution Prevention Program, "Automated DNA Sequencing," no date. As of March 19, 2010:
http://www.p2000.umich.edu/chemical_waste/cw12.htm

U.S. Department of Justice, DNA Initiative, "Steps in DNA Sample Processing," no date (published online with permission from *Forensic DNA Typing: Biology, Technology, and Genetics of STR Markers* [2nd Edition], written by John Butler of the National Institute of Standards and Technology and published by Academic Press, an imprint of Elsevier, New York). As of March 19, 2010:
http://www.dna.gov/basics/analysis/steps

U.S. Department of Justice, DNA Initiative, "STR Analysis," no date. As of March 19, 2010:
http://www.dna.gov/basics/analysis/str

U.S. Department of Justice, Federal Bureau of Investigation, *FY 2008 Authorization and Budget Request to Congress*, 2008.

U.S. Department of Justice, National Institute of Justice, *Understanding DNA Evidence: A Guide for Victim Service Providers*, 2001. As of March 19, 2010:
http://www.ncjrs.gov/pdffiles1/nij/bc000657.pdf

U.S. Department of Justice, National Institute of Justice, *Using DNA to Solve Cold Cases*, July 2002.

U.S. Department of Justice, National Institute of Justice, "Recommendation of the National Commission on the Future of DNA Evidence," November 13, 2007. As of March 19, 2010:
http://www.ojp.usdoj.gov/nij/topics/forensics/dna/commission/recommendation.htm

U.S. Department of Defense, *Biometrics Task Force Annual Report Fiscal Year 2008*, 2008.

U.S. Department of Defense, Defense Science Board, *Report of the Defense Science Board Task Force on Defense Biometrics*, March 2007.

"U.S. Secretly Collecting Detainee DNA," *UPI*, October 15, 2008. As of March 19, 2010:
http://www.upi.com/Top_News/Special/2008/10/15/US-secretly-collecting-detainee-DNA/UPI-27841224111989/

Willing, Richard, "DNA Backlog Piles Up for FBI," *USA Today*, September 3, 2007.

Woodward, John D., Jr., "The Law and the Use of Biometrics," in Anil K. Jain, Patrick Flynn, and Arun A. Ross, eds., *Handbook of Biometrics*, New York: Springer, 2008.