SUMMARY

INTRODUCTION

The U.S. Army has a growing need to control access to its systems in times of both war and peace. In wartime, the Army's dependence on information as a tactical and strategic asset requires the Army to carefully control its battlefield networks. From logistics flows to intelligence on enemy forces, the Army depends on confining access to its data to authorized personnel. This need for access control is also critical at the weapon system level.

Access control issues are important to the peacetime Army because improving the efficiency of peacetime operations, including controlling access to facilities, computer systems, and classified information, depends on fast and accurate identification. The Army also operates a vast set of human resource services involving health care, retiree and dependent benefits, and troop support services. These services create the need for positive identification to prevent fraud and abuse.

The use of biometrics has been proposed as a solution to these many needs. Biometrics are physical characteristics or personal traits of a person that can be measured and used to recognize that person either by identification or verification. Identification occurs when the biometric system identifies a person from the entire enrolled population by searching a database for a match. This process is sometimes called "one-to-many" matching. Verification occurs when the biometric system authenticates a person's claimed identity from his previously enrolled pattern. This is called "one-to-one" matching.

The potential of biometrics, combined with increased policymaker interest, has led the Army to undertake an intense assessment of biometric technologies. The Army is studying how it can use biometric applications to improve security, efficiency, and convenience, as well as whether it should establish an Army biometric center that could serve as a central data repository for biometric information and perform research, development, test, and evaluation (RDT&E) functions. Because interest in biometrics in the federal government is widespread, the Army is also examining the role a center could play in supporting a national biometrics program.

At the direction of Lieutenant General William H. Campbell, Director of Information Systems, Command, Control, Communications, and Computers (DISC4) and the Army's Chief Information Officer, RAND examined the legal, sociological, and ethical issues associated with the U.S. Army's use of biometrics and the establishment of an Army biometric center. RAND assembled an interdisciplinary team of researchers who reviewed literature and interviewed technologists, program managers, lawyers, ethicists, and privacy experts to identify issues and methods to address them. To test its conclusions, RAND conducted a workshop with a number of experts in mid-December 1999. The research, which focused on the United States, had the following four objectives:

- Provide an overview of biometric technologies.
- Identify sociocultural (meaning sociological, legal, and ethical) concerns that might be raised by Army use of biometrics and suggest solutions to mitigate these concerns.
- Analyze the feasibility of an Army biometric program, including a national biometric center and national data repository.
- Provide implementation recommendations for the Army, including suggested areas for further research.

OVERVIEW OF BIOMETRIC TECHNOLOGIES

In the context of this report, "biometrics" refer to commercially viable automated methods of identifying, or verifying the identity of, a living person in real time based on a physical characteristic or personal trait of the individual. This is commonly done by comparing a stored template (defined as a type of file record of a characteristic or trait) against a template of the live image captured through a sensor. While many possible biometrics exist, at least eight mainstream biometric authentication technologies have been deployed or pilot-tested in commercial applications in the public and private sectors. They are fingerprint, hand/finger geometry, facial recognition, voice recognition, iris scan, retinal scan, dynamic signature verification, and keystroke dynamics.

RAND researchers compared these eight mainstream biometrics by interviewing technologists, vendors, and program managers, as well as studying the technical literature. They discovered that the utility and effectiveness of a biometric depends largely on the specific purposes for which it is used. Biometrics also vary widely in terms of intrusiveness, robustness, and distinctiveness.

WHAT SOCIOCULTURAL CONCERNS ARE RAISED BY USING BIOMETRICS?

As with all identification techniques, biometrics carry the potential to reduce the anonymity of our actions. In the United States, privacy has a great deal of value for our society and culture, and this importance is reflected in our laws. Hence, a feasibility assessment of Army use of biometrics and the establishment of a biometrics center must take into account the sociocultural issues that such use might raise.

We identified three major categories of concerns associated with biometrics: informational privacy, physical privacy, and religious objections.

Informational Privacy

Informational privacy, or an individual's ability to control information about himself, dominated the concerns of the experts interviewed. Specific informational privacy issues include

- function creep,
- tracking of individuals' activities, and,

- misuse of data, including identity theft.

Function Creep, in the context of biometrics, means that biometric data originally collected for one purpose are used for other purposes. Although using data for other secondary purposes might be worthwhile, sociocultural issues arise when individuals are not informed of these new purposes and have not given their consent to the new use.

Tracking refers to the specific function creep involved when biometrics are used to monitor an individual's actions or to search databases containing information about these actions. If a person must use the same standardized biometric to participate in life's everyday activities, he leaves a detailed record behind. This concern raises the question of whether using biometrics increases the ability to track individuals, possibly without their knowledge or consent.

Misuse of Information, in the form of data representing an individual's biometric, is also a potential problem. For example, using a biometric identifier, much the way a Social Security number (SSN) is used, to link a person's medical information with financial data, raises concerns. Misuse also includes concerns about identity theft. Because they are unique identifiers, biometrics should make identity theft more difficult; nonetheless, biometric data can be stolen or copied when used in certain ways.

Physical Privacy

Physical privacy concerns include

- stigmatization,
- actual harm, and,
- hygiene.

Stigmatization refers to the perception that biometrics carries a stigma. For example, fingerprinting has a strong association with criminal activity. These perceptions vary widely across cultures.

Actual Harm refers to the fear of some individuals that biometric technologies will actually do them physical harm. We have found no evidence that biometrics actually cause physical harm.

Hygiene refers to the fact that some object to using biometric devices that require touching a surface, for example, fingerprinting and hand geometry, because doing so might transmit germs from other individuals.

Religious Objections

Religious objections have been raised by certain Christian sects based on the "Mark of the Beast" language in the Book of Revelation. Although the number of these dissenters is small, some members of the Army community may hold similar beliefs. Thus, the Army must be prepared to address such objections.

ARE SUCH SOCIOCULTURAL CONCERNS NEW IN DEALING WITH BIOMETRICS?

Sociocultural concerns about biometrics are both similar and dissimilar to existing concerns regarding other government data collection and management efforts. Moreover, many of these same sociocultural concerns apply to private sector use of biometrics. Function creep, tracking, misuse of information, and identity theft are all longstanding concerns about the collection and storage of personal information. The use of the SSN illustrates the problem of function creep. When the Social Security Act was passed in 1935, promises were made to the American public that the SSN would never be used beyond its stated purpose—that is, to administer social security assistance. Today, despite these early assurances, an individual's SSN is used for many purposes, both in the public and private sectors.

On the other hand, despite these similarities, biometrics raise some concerns not associated with traditional identifiers, such as a password. Because biometrics are limited in number—humans have one face, 10 fingers, two eyes—concerns arise that if the biometric identification information is stolen, the individual would be unable to replace the identifier, which is relatively simple to do with today's current personal identification numbers (PINs). In addition, biometric data might contain medical information or indicate changes in medical conditions. While this is not the case for biometrics in use today, the potential is worrisome, because it would change the information available to organizations using biometrics as well as expand possibilities for misuse. Also, the capability to track individuals is significantly greater with biometrics than with traditional forms of identification. This capability may generate its own demand for use, leading to function creep. For these and other reasons, biometrics could be perceived by some as a qualitatively different means of checking identity.

HOW CAN THE ARMY MITIGATE THESE SOCIOCULTURAL CONCERNS?

The Army can rely on existing policies and procedures to address many of these concerns. However, because biometrics involve new technologies and our society increasingly focuses on the impact of information technology on privacy, it would be prudent for the Army to take a broad and integrated approach to managing its response to these sociocultural concerns.

Relying on Existing Laws and Regulations

Among the laws and regulations concerning government use of personal information, the Privacy Act of 1974 is most prominent. The Privacy Act regulates the collection, maintenance, use, and dissemination of personal information by federal agencies, including the Department of Defense (DoD) and the Army. Among its provisions, the Act addresses individual concerns related to personal information provided to a government agency. For example, the agency must state the purpose for collecting the data, its intended use of the information, and its authority to collect the information.

As a general rule, the Privacy Act prohibits a federal agency from disclosing personal information without the consent of the individual providing the information. However, the Act contains many exceptions to this rule. While the Privacy Act specifies the legal minimum the Army must do to be in compliance, the Army might want to provide broader privacy protections for its biometrics program. For example, it could take the position that no biometric data in its charge would be shared, similar to the rule DoD has for protecting DNA samples in its human remains identification program.

The Privacy Act also requires federal agencies and officials to protect their databases from unwarranted disclosures. This requirement addresses some of the concerns about misuse of data and identity theft.

The Army has regulations in place to accommodate religious objections. These regulations could be used to address religious objections to the use of biometrics.

In a case that has important implications for the Army, the U.S. Supreme Court has addressed informational privacy from a constitutional perspective. In *Whalen v. Roe*, the Court upheld a New York state law establishing a centralized computer database in which the state recorded and stored the names and addresses of all persons who obtained certain drugs pursuant to a doctor's prescription. The Supreme Court explained that New York had demonstrated its need for the database as part of its war on drugs and had taken extensive measures to prevent unauthorized disclosure of the data.

Similarly, the judiciary has addressed privacy concerns in related contexts. For example, the courts have consistently upheld federal, state, and local requirements for fingerprinting for employment and licensing, provided a rational basis existed for the requirement. Likewise, when a biometric is needed from an individual for a criminal justice purpose, the Army should be able to satisfy the constitutional requirements.

Taking a Broader, More Integrated Approach

No significant legal obstacles to Army use of biometrics in the United States have been identified. While the Army could rely on existing laws and regulations to provide a minimum level of privacy protection, the Army should take additional steps to strengthen privacy protections because it is in its best interest to do so. These additional steps include taking a broader, more integrated approach to mitigating sociocultural concerns. Such an approach includes four elements.

Step One: Thoroughly Explain Why Biometrics Are the Best Solution to a Particular Problem. This step requires a detailed statement of the problem, a description and evaluation of possible solutions, and a comparison of biometric capabilities to those of other potential solutions. This analysis will form the basis for individual and societal decisionmaking, balancing the benefits of biometrics against potential losses of privacy.

Step Two: Structure a Program and Select Technologies to Minimize the Effects on Privacy. This step will help prevent privacy concerns from arising. Within the constraints of meeting operational needs, Army decisionmakers should also consider the following:

- *Policies about sharing data* should be carefully designed to avoid perceptions of function creep and the development of tracking capability.
- *Privacy enhancing solutions* should be considered when the Army chooses biometric technologies. Specific examples that may allay privacy concerns about tracking include decentralizing template storage and matching; using nonforensic biometrics; using multiple biometrics; and using verification rather than identification applications. In addition, biometrics that are less intrusive or provide no medical information would likely be preferred by those concerned about privacy.
- *Data repository* choices affect perceptions of security and privacy. Holding template data on a smart card in the possession of the individual or locally with the sensor, rather than in a central repository, makes function creep and tracking less feasible.

Step Three: Educate the Army Community and the Public About the Purpose and Structure of the Program. Such an education program should explain what steps the Army has taken to ensure that privacy is protected. A campaign directed at both the Army community and the general public could generate support for the Army's program. The following questions should be addressed:

- What is the purpose of the biometric program? Who is included in it?
- What information will be available through the biometric?
- How will that information be used and who will have access to it?
- How will that information be protected?

- Who will establish, control, and review these practices?

Step Four: Assign Responsibility Within the Army for Guiding Steps One to Three. This step is important to ensure that sociocultural concerns are adequately addressed as the program is developed and implemented and as issues arise in the future.

WHAT IS THE FEASIBILITY OF AN ARMY OR NATIONAL BIOMETRIC CENTER?

Establishing an Army biometrics center, including both an RDT&E center and a central repository, has a good chance of success if it is based on justifiable program needs and structured to provide meaningful privacy protection. While legal, regulatory, technical, operational, security, and administrative issues affect how such a center could be established and what it could do, these do not impose overwhelming obstacles. However, a center may raise sociocultural concerns about privacy, with particular attention focused on a central repository. Concerns about a repository are likely to be much more sensitive to size, to purpose, and to who is in charge. While establishing a central repository could be justified based on particular purposes, it does not seem critical to the RDT&E effort. A centralized repository could help a test center verify the uniqueness of particular biometrics and algorithms by giving it large numbers of templates to compare, but this is only one of the activities that might be performed at an RDT&E center. In addition, biometric data are electronic records and could be sent relatively easily from one location to another. Thus, in this section, we address the RDT&E center and repository separately.

An *RDT&E center* could be justified by the need to focus activities in areas of interest to the government and to provide a forum to share information and coordinate activities across a number of organizations. While field or pilot testing and scenario evaluations are costly, they are the only reasonable methods to test a biometric system fully and reliably for deployment. Laboratory testing could be used to test algorithms and as an initial pass/fail test for biometric devices to achieve minimum standards for additional operational testing. An R&D lab could also undertake further development of mathematical and statistical methods for test design and evaluation of biometric systems. An R&D center could be a source of advice on biometric systems for agencies internal and external to the Army. It could advise other agencies regarding technology considerations and help them develop educational roll-out pieces for their biometric programs. Whether the Army would seek the role of center coordinator depends on the importance biometrics are expected to have in the Army. Whether this should be a truly national center or an Army or DoD center depends on the importance of biometrics to the nation at large.

A *central repository* will raise more sociocultural concerns. The explanation about why such a repository is needed should adhere closely to the points raised earlier about defining the purpose—explaining what the data will be use for, what additional data will be stored with the templates, who can access the data, and how data will be protected—and deciding who oversees these processes. Concerns about the repository are likely to depend on whose biometric identification information is included (e.g., only service members or also Department of the Army civilians, contractors, retirees, dependents, and foreign nationals).

A central repository could be justified by the need to use an identification biometric for the Army rather than simply relying on verification. Or, it may be necessary to have a centralized verification location so that certain identifiers can be used in multiple locations. A centralized repository could also help a test center verify the uniqueness of particular biometrics and algorithms, giving it large numbers of templates to compare.

A *national biometric center* must be justified in the same way by those most interested in having such a center. It is not clear that those most interested in RDT&E will also be most interested in a repository. While the military might want to move the technology forward, perhaps law enforcement or social service agencies will have the greatest interest in establishing some form of national repository for biometric data. These other agencies are probably most interested in comparing data to search for fraud or criminal evidence, activities likely to meet with sociocultural objections. An Army-run national biometric repository might not have such strong interests in sharing data with other agencies, although it would likely be under pressure to do so.

CONCLUSIONS AND RECOMMENDATIONS

Based on our analysis, we have identified no significant legal obstacles preventing the Army from establishing a biometrics program in the United States. Although some sociocultural concerns may arise, particularly with regard to privacy issues, these can be addressed, albeit minimally, by existing Army regulations, particularly those relating to the Privacy Act. To demonstrate its commitment to privacy, the Army should consider providing additional protection for its biometric databases beyond the requirements of the Privacy Act. In particular, the Army might want to place strict requirements on sharing biometric data with other agencies and organizations. If other agencies believe they have a legitimate claim to access to the Army's data, it might be better for Congress or the White House to decide this issue through the political process.

The Army should provide a detailed analysis of the problems that biometrics can help solve. This should include a detailed description of the problem, a description and evaluation of possible solutions, and a comparison of biometric capabilities to those of other potential solutions. This analysis will form the basis for individual and societal decisions balancing the benefits of biometrics against potential losses of privacy.

Although a central repository may be necessary, it should be justified in the same way as the Army biometric program, by establishing the need for a center based on specific problems to be addressed. The size and functions of this center will contribute to public perceptions and concerns about its purposes and potential threats to individual privacy.

Carefully targeted research could help the Army address sociocultural concerns when implementing its biometrics program. Greater Army participation in the U.S. government's Biometric Consortium could also assist Army and DoD research interests. As the Army uses biometrics overseas, it must consider international law issues. Moreover, the Army could benefit from research evaluating whether biometric data implicate medical information of any kind.

As this report was being prepared for final publication, Deputy Secretary of Defense Rudy de Leon issued a memorandum on December 27, 2000, consolidating oversight and management of biometric technology under the recently created DoD Biometrics Management Office (BMO). This memorandum also called for the formal establishment of a DoD Biometrics Fusion Center (BFC) under the BMO. The BFC's purpose is to acquire, test, evaluate, and integrate biometrics and to develop and implement storage methods for biometrics templates. The BFC is located in Bridgeport, West Virginia.

This memorandum derived from Public Law 106-246, signed by President Clinton on July 13, 2000, which included the following provision: "To ensure the availability of biometrics technologies in the Department of Defense, the Secretary of the Army shall be the Executive Agent to lead, consolidate, and coordinate all biometrics information assurance programs of the Department of Defense."[1]

As the DoD BMO and the Army, as executive agent, continue to assess biometrics, they must carefully consider the sociocultural concerns biometrics raise, along with technical, operational, security, bureaucratic, and administrative issues.

[1] For more information about the DoD Biometrics Management Office, please visit the DoD BMO Web page, available at http://www.c3i.osd.mil/biometrics/.