RAND Arroyo Center
ARMY RESEARCH DIVISION
Research Brief

Can Biometrics Help the Army Solve An Identity Crisis?

The Army is having an identity crisis, and it affects both its wartime and peacetime operations. Simply put, the Army needs to ensure that the right people—and only the right people—can get access to its information systems, its weapons, and its many databases that serve the Army community. Biometrics—that is, physical characteristics or personal traits that can be measured quickly—may offer a solution. But using biometrics raises some knotty legal, ethical, and sociological issues—for example, how to safeguard biometric information so it cannot be used for other, possibly nefarious, purposes. The Army has been studying these issues and has been considering the feasibility of establishing a biometric research center that could serve as a central data repository and carry out test and evaluation.[1]

The Army asked RAND's Arroyo Center to help it come to grips with these issues. The results of the Arroyo Center work have been published in *Army Biometric Applications: Identifying and Addressing Sociocultural Concerns*. Major conclusions of the research include the following:

- No significant legal obstacles bar the Army from establishing a biometrics program in the United States.
- Valid sociological concerns exist, particularly in the area of privacy, but these can be addressed by existing Army regulations (minimally) and by installing additional safeguards.
- A centralized repository for biometric data may be necessary. However, the size and functions of such a center could easily fuel public concerns over privacy and other issues. Therefore, the need for it must be justified by a careful analysis of the problems to be addressed.

WHAT BIOMETRIC TECHNOLOGIES ARE AVAILABLE AND WHAT CONCERNS DO THEY RAISE?

Many biometrics exist, but eight primary ones have been either used or tested in both public and private settings. The most familiar (and longest used) biometric is the fingerprint. Others include hand (or finger) geometry, facial and voice recognition, iris and retinal scan, signature verification, and keystroke dynamics. With varying degrees of certainty, all can identify a specific individual. However, they also vary in their intrusiveness, the degree to which the public accepts them, and the types of issues they raise. The Arroyo Center research identified three major categories of concern: information privacy, physical privacy, and religious objections.

Information Privacy

By far the greatest concern was about an individual's ability to control personal information. Not surprisingly, misuse of the information ranked high on the list of information privacy issues. Widely publicized accounts of identity theft and financial loss stemming from it have made people nervous about any information that could enable someone to assume their identity. Biometric data, though more complex than most passwords, can also be stolen or copied, so any attempt to develop a system using it must take these concerns into account.

[1]The Army's biometric work has assumed more importance since it has been designated the Department of Defense Executive Agent for biometrics used for information assurance. To learn more about the DoD program, see their Web page at www.c3i.osd.mil/biometrics.

Misuse is not the only information privacy concern. Some worry about "function creep"—that is, using information collected for one purpose to do something else. These secondary purposes may be perfectly valid, but if people have not been informed about the new use and have not consented to having information about them applied to it, they could object. Another worry is that biometric information will enable a third party to track an individual's actions or search databases to get information about them. Using a biometric to participate in routine daily activities (e.g., entering or exiting buildings, making financial transactions) leaves a detailed record. This capability bothers many people, who worry that some biometrics may allow their activities to be monitored without their knowledge or consent.

Physical Privacy

Unlike some other identifiers—a Social Security number, for example—biometrics raise issues of physical privacy. One is that certain biometrics carry a stigma. Fingerprints, for example, are widely associated with criminal activity. Another issue is concern about actual physical harm. While the research team found no biometric that causes such harm, it nonetheless troubles some. For example, retinal scanning techniques require individuals to place their eyes close to a camera lens, a requirement that makes some people uneasy. Hygiene issues also concern some. The need to place a hand or finger on a sensor plate can prompt fear about the spread of disease.

Religious Objections

Certain Christian sects have objected to the use of biometrics based on the "Mark of the Beast" language in the Book of Revelation. Although the number of such believers is relatively small, some members of the Army community might hold similar beliefs. The Army needs to be prepared to address such objections.

HOW CAN THE ARMY MITIGATE CONCERNS?

Many of these concerns are not new, and the Army has rules and regulations in place to address them. However, widespread use of biometric technologies is new, and the Army should review its current policies and regulations to ensure that they address the concerns people have.

The Privacy Act of 1974 is the most prominent piece of federal legislation governing the use by the federal government of personal information. Generally, the Act precludes the federal government from disclosing personal information without the consent of the person who provided it. It specifies the minimum that the Army must do to protect the information, but the Act contains many exceptions.

The Army could rely on existing law and regulation to protect any biometric data it might collect, but it may wish to take a broader and more integrated approach. A first step would be simply to explain thoroughly why a biometric is the best solution to a given problem. A full understanding of the issues, including costs and benefits, could help the program win acceptance. If, for example, the Army wished to substitute fingerprint recognition for computer and database passwords, it might highlight the problem of lost, forgotten, or purloined passwords. On the positive side, it could emphasize the convenience and elimination of the need for periodic password changes.

As a second step, the Army could structure the program to minimize the effect on privacy. To allay the sorts of concerns described above, the Army might want to do more than the minimum. It could, for example, establish a policy that its biometric information would not be shared with any other organization, similar to the rule that the Department of Defense has for protecting DNA samples it has collected as part of its program to identify human remains. Establishing policies about sharing data from the outset, decentralizing storage locations or storing the data with the individual (e.g., on a smart card) could alleviate many concerns.

A third step would involve a vigorous education program. Such a campaign, aimed at soldiers, family members, and the public, could not only allay fears, but it could also build support for the program. Finally, the Army should assign clear responsibility for each step outlined above.

A BIOMETRIC CENTER IS FEASIBLE

From a sociocultural perspective, it is feasible for the Army to establish a center to store biometric data and test and evaluate biometric technologies. Among the legal, technical, regulatory, operational, and security issues that must be addressed, the most sensitive aspect of such a center is the repository component, particularly its size, purpose, and organizational assignment. Concerns over these issues are likely to depend on whose information is included in it (e.g., servicemembers only, Department of Army civilians, contractors, retirees, dependents), what

purposes the information serves (e.g., benefit eligibility, installation access), and who has access to it (e.g., other services, law enforcement agencies).

WHAT SHOULD THE ARMY DO?

As the Army continues its study of biometrics and their applicability to its needs, it should consider the following:

- Demonstrating its commitment to individual privacy by placing strict limits on sharing biometric data with other organizations.
- Providing a detailed analysis of the problems that biometrics can help solve.
- Justifying any central repository in the same way it justifies its biometric program.
- Participating in the U.S. government's Biometric Consortium.
- Exploring the issues of international law that might affect implementation of a biometric program overseas.

RAND research briefs summarize research that has been more fully documented elsewhere. The research summarized in this brief was carried out in the RAND Arroyo Center; it is documented in Army Biometric Applications: Identifying and Addressing Sociocultural Concerns, *by John D. Woodward, Jr., Katharine W. Webb, Elaine M. Newton, Melissa Bradley, and David Rubenson, MR-1237-A, 2001, 215 pp., ISBN: 0-8330-2985-1, available from RAND Distribution Services (Telephone: 310-451-7002; toll free 877-584-8642; FAX: 310-451-6915; or email: order@rand.org). Abstracts of RAND documents may be viewed at www.rand.org. Visit the Arroyo Center at www.rand.org/ard. Publications are distributed to the trade by NBN. RAND® is a registered trademark. RAND is a nonprofit institution that helps improve policy and decisionmaking through research and analysis; its publications do not necessarily reflect the opinions or policies of its research sponsors.*

RAND

1700 Main Street, P.O. Box 2138, Santa Monica, California 90407-2138 • Telephone 310-393-0411 • FAX 310-393-4818
1200 South Hayes Street, Arlington, Virginia 22202-5050 • Telephone 703-413-1100 • FAX 703-413-8111
201 North Craig Street, Suite 102, Pittsburgh, Pennsylvania 15213-1516 • Telephone 412-683-2300 • FAX 412-683-2800

RB-3024-A (2001)