Chapter One

INTRODUCTION

BACKGROUND

The U.S. Army has a growing need to improve access control for its many systems, both in wartime and in peacetime. In wartime, the Army's dependence on information as a tactical and strategic asset requires it to carefully control its battlefield networks. From information on logistics flows to intelligence on enemy forces, the Army depends on confining access to its data to authorized personnel.

Access control is critical for weapon systems. These systems increasingly consist of physical, logical (computer), and informational components. Army weapon systems are so powerful and often so dominant that unauthorized use of even a single system can have significant adverse consequences. Moreover, if an enemy were to capture an Army weapon system with inadequate access control measures in place, the enemy could use the captured resource to its advantage.

In peacetime, access control issues are also important because improving the effectiveness and efficiency of Army operations depends on fast and accurate identification of authorized users. Examples include controlling access to facilities, computer systems, and classified information. Moreover, the Army operates a vast set of human resource services, involving health care, retiree and dependent benefits, troop support services, and many others. Access control is important in these systems to verify claims for benefits and to reduce fraud.

Biometrics is a possible solution for dealing with the Army's access control problems. Biometrics use distinctive physical characteristics

or personal traits, such as fingerprints or hand geometry, to make nearly instantaneous verifications of claimed identity or to identify individuals. The push for biometrics is driven by both its technical possibilities and political interest.

From a technical point of view, commercially viable biometric authentication systems are in full-scale operation. Significant optimism has been expressed that technological improvements will lead to better, faster, less costly, and more pervasive systems. Because biometrics are an integral part of human beings or "bar codes for the body," they offer a convenience and efficiency that other identifiers, which must be remembered or produced, do not. For this reason, biometrics are seen as a means of enhancing security for activities currently protected by traditional means of access control—cards, personal identification numbers (PINs), and passwords.

Biometrics can also be used in conjunction with cards and PINs to enhance security. In many applications, a biometric could replace the card or PIN entirely. If there are no cards to lose or numbers to remember, in many cases biometrics will reduce operational and administrative costs and increase user convenience.

Some experts contend that biometrics, if properly used, could enhance privacy, along with security and convenience, by allowing for an individual's identity to be secured by different biometrics.[1] In other words, the use of multiple biometrics is the equivalent of an individual being issued multiple PINs or passwords, with the critical difference being that biometric-based systems provide better security and greater convenience. From the privacy-enhancing perspective, compartmentation, or the separation of personal information into small parts, is best achieved by the use of multiple biometrics.

Many public sector organizations use biometrics widely. For example, the U.S. Immigration and Naturalization Service (INS) currently makes the most extensive use of biometrics of all federal agencies.[2]

---

[1] See, e.g., Wayman, (1998). The use of multiple biometrics is sometimes referred to as "biometric diversity" or "biometric balkanization."

[2] See Appendix B, Program Reports. See also Wayman (2000). The INS Web site with public information regarding the use of one of its most popular biometric programs, known as the U.S. INS Passenger Accelerated Service System (INSPASS) is available at http://www.ins.usdoj.gov/graphics/howdoi/inspass.htm.

Other federal agencies using biometrics include the Federal Bureau of Investigation (FBI), the Federal Aviation Administration (FAA), and the Department of State and the Department of Defense (DoD). State social services programs use biometrics to reduce fraud and to enhance the convenience of these programs. Many state and local law enforcement agencies digitize fingerprints to speed criminal investigations and background checks. President Bill Clinton, in his 2000 State of the Union Address, and other political leaders have expressed interest in so-called "smart gun" technologies.[3] A smart gun could feature a biometric, such as a fingerprint, as an integral part of the firearm to make certain that only the authorized firearm user could fire the weapon. The private sector's growing interest in biometric applications stems as much from perceptions of increased efficiency and convenience as from increased security. In the Army, as in civilian life, biometrics are expected to be useful in many different applications.

Policymakers are also a driving force for those who view biometrics as a potential solution to the Army's access control problems. In 1999, Congress included $10 million in the Army's budget to study biometrics, specifically instructing the Army to conduct:

> [A]n immediate assessment of biometrics sensors and templates repository requirements and for combining and consolidating biometrics security technology and other information assurance technologies to accomplish a more focused and effective information assurance effort. (U.S. Senate, 2000)[4]

---

[3]See Clinton (2000). President Clinton stated:

> Technologies now exist that could lead to guns that can only be fired by the adults who own them. I ask Congress to fund research in smart gun technology. I also call on responsible leaders in the gun industry to work with us on smart guns and other steps to keep guns out of the wrong hands and keep our children safe.

See also LeDuc and Whitlock (2000) (reporting that Maryland Governor Parris Glendening is proposing to spend $3 million over the next three years to fund smart gun research), and Sinatra (2000).

[4]Public Law No: 106-79, Oct. 25, 1999. See also Byrd (1999), noting that "the Army has exhibited strong leadership in the exploration and development of technologies in the biometrics arena and is a natural leading candidate to be considered as the executive agent in this work for the Department of Defense and perhaps the federal government."

An important component of determining the feasibility of an Army biometrics program along the lines envisioned by Congress, is understanding what sociocultural (meaning sociological, legal, and ethical) concerns will be raised by Army use of biometrics and how the Army can best respond to these concerns. As with so many government-mandated programs, the use of biometrics requires tradeoffs between individual rights and societal needs.

Sociocultural concerns are usually among the first to emerge during periods of change, particularly in response to an emerging technology, such as biometrics. Our societal code of ethics helps us adjust, or not, to the changes and challenges posed by a new technology. In the case of biometrics, many of these sociocultural concerns involve the appropriate protections of individual rights related to informational privacy, physical privacy, and religious beliefs. As the law mirrors the society that creates it, legal responses to such sociocultural concerns follow the sociocultural changes. These responses can include the enactment of new statutes or regulations, changes to existing ones, or the adoption of new codified restraints on behavior.

OBJECTIVES

As part of its response to the congressional directive to evaluate the feasibility of an Army biometrics program and center, Lieutenant General William H. Campbell, the Director for Information Systems, Command, Control, Communications, and Computers (DISC4) and the Army Chief Information Officer, asked RAND in October 1999 to review current commercially viable biometric applications and assess the sociological, legal, and ethical issues raised by Army use of biometrics, including establishment of a biometrics center.

APPROACH

To review commercially viable biometric applications, the RAND biometrics team consulted numerous paper and on-line publications and Web sites, interviewed more than 50 biometric experts in both the public and private sectors, and participated in several conferences at which a number of biometrics programs were presented. In sum, we reviewed approximately 50 biometric initiatives.

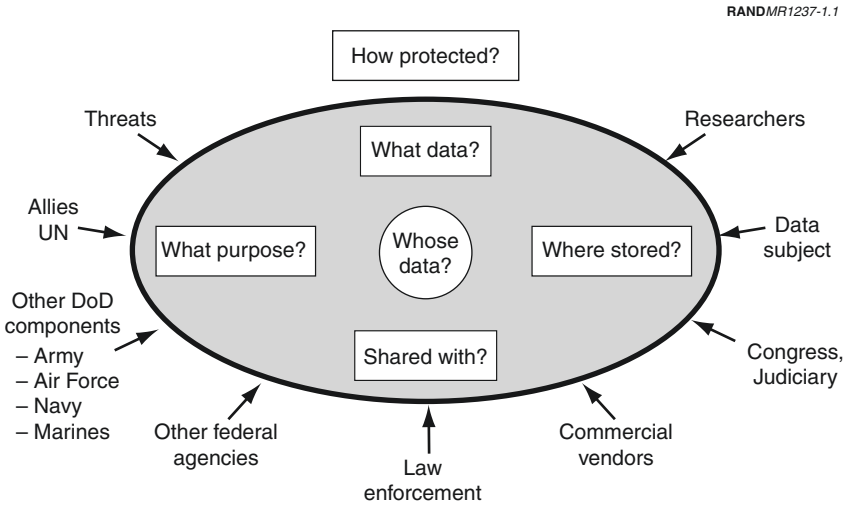

Figure 1.1—Dimensions of the Issues About Army Use of Biometrics

RAND assembled an interdisciplinary team to assess the sociological, legal, and ethical issues associated with biometrics and to develop a set of hypothetical issues that could stem from an Army biometrics program. We noted from the start the overlap among these areas and the important linkages between sociological, legal, and ethical issues. Figure 1.1 illustrates the dimensions of the issues raised and explored during our research.

To answer the many questions initially posed, we interviewed technologists, lawyers, ethicists, and privacy experts about individual rights and the interplay of law and technology. We also studied other biometric programs that would offer insights for how the Army community, consisting of servicemembers, Army civilians, contractors, Army retirees, and dependents, might respond to programs using biometrics.[5] In addition, we used information gleaned during our applications assessment to address some of our questions related to the capabilities of biometric technologies and, hence, the implications of the technologies for individuals and society.

[5]See Appendix B, which discusses a number of programs reviewed by RAND.

To test the results, RAND conducted a workshop in December 1999 with approximately 25 experts, including technologists, lawyers, ethicists, privacy advocates, medical doctors, biometric program managers, research scientists, and law enforcement professionals. The workshop used a scenario approach to explore concerns related to government-mandated compliance with a biometrics program. This approach focused on concerns that an individual might raise as well as measures the Army might take to mitigate these concerns. For example, an individual's concern about whether his biometric data is protected from unauthorized disclosure could be addressed by a comprehensive plan for database security. The workshop helped establish basic guidelines for designing and implementing a biometrics program, a research development, test, and evaluation (RDT&E) center, and, if necessary, a central repository for biometric data.

SCOPE

Although our approach was thorough, we recognize that our research had some limitations. First, our approach did not fully capture the views of every societal group. Second, our approach did not systematically survey the Army community, all of whom might be included in a biometric program. This issue is addressed again in Chapter Six where we discuss conclusions and recommendations. Third, our research focused primarily on the sociological, legal, and ethical issues of implementing an Army biometrics program in the United States. However, we are aware that foreign cultures and international legal systems will have different and perhaps contentious views of some of the issues we raise. While we briefly discuss European Union privacy laws in our legal assessment (see Appendix C), a systematic survey of the sociocultural concerns of individual nations and regional organizations is beyond the scope of this report. This issue is addressed further in our conclusions and recommendations.

ORGANIZATION OF THE REPORT

Following a brief overview of biometrics in Chapter Two, we use the next three chapters to answer three fundamental questions:

- What sociocultural concerns does the use of biometrics raise and how are these concerns different from those related to the use of other identification methods?
- What actions can the Army take to address these concerns?
- What is the feasibility of a national biometric center?

We finish the report with conclusions and recommendations that draw on our answers to these three questions.

We also include five appendices providing additional background material. Appendix A provides more detail on biometric technologies. Appendix B presents the experiences of some private and public sector biometric programs. Appendix C is a detailed review of the legal issues surrounding Army use of biometrics. Appendix D provides information on the U.S. government's Biometric Consortium, and Appendix E lists the names of the participants and organizations interviewed for the project.