Chapter Six

CONCLUSIONS AND RECOMMENDATIONS

In this chapter, we draw on the discussion in the previous five chapters to present our conclusions and recommendations.

CONCLUSIONS

RAND identified three potential sociocultural concerns with biometrics related to informational privacy, physical privacy, and religious objections.

With respect to informational privacy, laws, such as the Privacy Act of 1974, and regulations, such as the Army Privacy Program, provide a baseline for protecting an individual's privacy interest in his personal information. The Army has flexibility to either accept these standards as the maximum privacy protection it will give to individuals or provide additional protections beyond the Act's requirements, particularly with respect to limiting the sharing of biometric data.

As for physical privacy, the courts have generally upheld federal, state, and municipal statutes requiring fingerprinting as a condition of employment and licensure. Accordingly, the Army appears to face no significant legal obstacle in this regard, although it might have practical concerns if biometrics make people so uncomfortable they avoid or sabotage the system or complain to their elected officials, for example.

With respect to religious concerns, the Army already has in place detailed regulations to address conflicts between an individual's religious practices and Army procedures.

Thus, although the use of biometrics raises sociocultural concerns, based on today's perceptions of biometrics these concerns present no serious obstacle to proceeding with an Army biometrics program, provided the Army addresses the concerns in accordance with existing laws and regulations.

How the Army addresses these concerns will have an impact on how well its biometrics program is received. Simply following the letter of the law may be sufficient for a narrowly defined biometrics program, such as one designed to protect battlefield intelligence nodes. However, should the Army determine that biometrics are a viable solution for Army, DoD, or national information assurance needs, greater efforts to allay concerns will become important. The larger the population included in the Army's biometrics program, the larger the likelihood that some will object on informational privacy, physical privacy, or religious grounds.

Finally, as an emerging technology, biometrics are changing rapidly. While biometrics do not currently provide medical information, this might change as new biometrics become commercially viable or researchers begin to test whether certain biometric templates could be somehow linked to particular medical conditions or diseases. For example, DNA analysis may become automated to the point that it becomes feasible to use a DNA-based biometric in the authentication applications discussed in this report. Because of DNA's close association with medical information, mandated participation in a DNA-based biometric program is likely to be controversial in the Army community and the general public.

Because biometrics are rapidly changing technologies, society's views of information technology will also develop. The impact on biometrics of increased societal experience with computers, cyberspace, electronic commerce, the digitized world, and the Internet could cut either way, reducing concerns about biometrics or heightening public interest in greater privacy protection. The Army could be forced to address these spillover effects in the future.

RECOMMENDATIONS

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. They should specifically consider the following recommendations, which address how the Army (and the BMO) should implement its biometrics program as well as identifying issues that the Army and BMO should explore. We begin by focusing on implementation.

Incremental Implementation

Based on current Army use of biometrics, it is not clear that the establishment of a national RDT&E center or a biometric data repository is necessary. The Army's biometric interests will best be served by an incremental approach to building a biometrics program and establishing a data repository.

This incrementalism need not limit the Army to a few applications or participants. Rather, it suggests that the Army should take a purposive approach, defined as focusing its biometrics efforts on specific problems the Army wants to solve and on specific purposes the Army wants to achieve. A purposive approach suggests that the Army

---

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

might want to try many biometric pilot programs and tests involving different biometric technologies to help it determine what works best for solving a particular problem and achieving a certain purpose. Along these lines, the Army would likely benefit from greater participation in the U.S. government's Biometric Consortium, the federal focal point for much biometric research and development.[2]

If this purposive approach generates the need for an RDT&E center or a central repository for biometric data, then the Army will be on firm ground as it moves to establish these activities whether for the Army only or for DoD as a whole. A decision designating the Army as the federal government's executive agent of a national biometric center should be made only after careful consideration. If made prematurely, such a decision is likely to raise more questions for the Army than the Army is prepared to address as well as tax its bureaucratic resources to answer the questions.

Finally, as the Army implements biometrics programs, it will want to proceed with additional care when expanding the programs to include foreign citizens, whether they are employees on U.S. bases overseas or allies fighting on our side. The sociological and legal issues raised in this context may be more complicated to address than those related to U.S. citizens.

Privacy Act Implications

It is not clear that the Army's broad interests in providing for the nation's defense are significantly enhanced by sharing biometric information in its charge with other agencies, even if the other agencies' uses are also in the national interest. We believe the Army can gain much and lose little by taking an approach that protects the privacy of the Army and DoD communities in their biometric data. As a starting point, the Army should place strict limits on the sharing of biometric data. These limits should go beyond the minimum protections of the Privacy Act. The Army's approach to sharing biometric data should be that such data should not be shared unless the sharing is directly related to the purpose for which the biometric was taken. If other agencies believe it imperative for them to have access

[2]See Appendix D for a discussion of the Biometric Consortium.

to the Army's data, they should make their case to Congress or the White House about why they should be able to access it.

Education

The Army's biometrics program—whether it includes a collection of small, discrete programs; an Army-managed RDT&E center; or a centralized data repository—should be discussed publicly. The Army must assure participants, policymakers, and the public that biometrics are necessary to the Army's needs and that the technology's benefits outweigh any individual costs.

An education campaign will be important to gaining support from participants in the Army community and protecting the Army's program from critics on the outside. A comprehensive threat analysis is critical to the education campaign because it will help the Army make its case as to why the Army needs to use biometrics. Additionally, the Army's education campaign must reflect a thoughtful data-sharing and safeguarding program. If the Army believes it needs to use biometrics on a large scale, then it must work to be a model for the rest of government. It cannot afford to be an example of how not to do a biometrics program.

Choosing Technologies

The Army should consider the sociocultural concerns identified in this report when it chooses biometric technologies and designs biometric system architectures. In some cases, the biometric choice and system architecture design, including decisions about where the Army will locate template databases, can be made with the objective of enhancing privacy. A common concern is that locating template databases in a central repository and frequently transferring data from the field increases the system's vulnerability to hackers. This potential vulnerability may be avoided in part by decentralizing template storage and matching. For example, the Army's biometrically protected smart card at Fort Sill, where the biometric measured could be found only on the card, provided privacy protection for the participants. Similarly, the use of multiple biometrics or biometric diversity protects privacy because it makes for compartmentation.

The Army's selection of a biometric will be purpose driven. However, the Army will be better off avoiding biometrics that also contain additional information unless the threat analysis demands this type of biometric. Thus, even if a DNA-based biometric becomes commercially viable, we would discourage the Army from deploying it because of the associated concerns it raises about genetic information. In sum, as the Army chooses technologies it will also want to consider their effect on privacy concerns and societal perceptions, as well as their benefits for addressing a particular threat.

Implementation Oversight

As the Army pursues biometrics, it might want to establish a board or committee to assist with implementation. Such a board may be useful to screen requests for the sharing of biometric information, to develop data-safeguarding and data-destruction policies, to track biometric use in the Army and DoD communities, and to provide other oversight as required. The Army should develop an institutional asset that monitors Army biometric programs, including pilot programs and experiments. Ensuring procedural consistency would also help address sociocultural concerns. The board would help the Army maintain awareness and attentiveness to new concerns that might be raised about biometrics.

Additional Issues

As discussed more fully in Appendix C, the European Union (EU) Data Protection Directive has the potential to raise issues affecting the Army's use of biometrics in EU member states, whether on U.S. military facilities or in different settings. The Army should explore further the directive's implications and continue to monitor the implementation of the directive's compliance scheme. In particular, the Army should monitor the implementation of the "safe harbor" principles, which provide U.S. organizations with a means of satisfying the directive's requirement for "adequate" privacy protection. The Army should also pay close attention to how the directive's various exceptions and exemptions are interpreted because the scope of these exceptions may affect U.S. interests.

The Army has operations in many foreign countries at any given time. From the international perspective, the Army must be mindful of the sociocultural concerns raised by Army use of biometrics in foreign settings. As Army biometrics applications move overseas, research on the likely sociocultural concerns of foreign countries and regional organizations will need to be done. However, the Army would find the results of such research more useful if it specifies the purpose of the biometric program, the candidate biometrics, the foreign location, and who the Army wants to participate (e.g., foreign military personnel and/or civilians).

Concerns have also been raised about the need for systematic assessment of the Army community to better understand its views on biometrics. Because such assessments depend so much on the specific problem the biometrics are being used to address—i.e., their purpose, methods of using and safeguarding data, and who is to be included in the system—we believe it would not be productive to poll the Army community until a specific application is in mind. However, as part of a purposive approach to biometrics, the Army should use sociological research technologies to test receptivity to biometrics. As biometrics are identified as solutions to particular problems, it would be more useful to engage focus groups to gauge how biometrics will be received and to help educate potential participants.

The Army might support research on whether biometric templates contain medical information, whether they might in the future, and whether the information would be provided inherently in the biometric (as with DNA) or by inference (as with retinal scans that show changes that a medical professional might further research and interpret).

Finally, we stress that all of this analysis depends on the Army's explanation of its problems and how biometrics can fix these problems. The Army's explanation must be more than just a statement that the Army needs improved access controls to enhance the security of its informational and physical assets. The Army must explain the weaknesses of the current systems, options to address these weaknesses, and how biometrics can solve the problems. Such an analysis is critical to providing the basis for the Army community, policymakers, and the public to determine whether concerns about biometrics are outweighed by the benefits they bring.