Chapter Five

WHAT IS THE FEASIBILITY OF A NATIONAL BIOMETRIC CENTER?

As noted in Chapter One, biometrics are a potential solution to Army needs. However, the findings of the previous two chapters indicate the Army must justify its program based on specific problems for which specific biometrics are an appropriate solution. As shown in Chapter Four, the feasibility of a biometrics program rests on how the program is structured and whether its implementation adequately addresses concerns about informational privacy, physical privacy, and religious objections as identified in Chapter Three. The establishment of a biometrics center, to include an RDT&E facility and a repository has a good chance of success if it is justified by program needs and structured and managed to provide the greatest privacy protection possible.[1]

The question for the Army is what kind of center makes sense for the Army to operate. A center could focus on RDT&E exclusively or include a repository where templates would be stored. Along these lines, the center's role could range from a very modest RDT&E facility with no template repository that would serve Army needs exclusively to a larger Army-operated center playing the lead role for DoD to a truly national center that would include RDT&E and a template repository that could be the focal point of all the U.S. government's biometrics work.

[1] In researching and writing this chapter, the authors relied heavily on the following sources: Newton and Rubenson (1999), Newton and Webb (1999), and Wayman (1999c).

Based on our analysis, we find that unless significant benefits to the Army are associated with running a national biometric repository, taking on this challenge, particularly at the beginning of the Army's foray into biometrics, runs the risk of raising concerns that could threaten the entire program. However, a biometrics RDT&E center, if warranted by Army needs, could be led by the Army without the sociological, legal, and ethical concerns related to the running of a repository.

In either case, education of the public is critical to success. The establishment of a center, whether for RDT&E or a data repository, is not a program to just be "slipped into" legislation. Particularly in the case of a large-scale data repository, the Army must make a compelling argument for managing such a repository. To do this, it must be able to provide convincing answers to the five questions raised in Chapter Four.

- 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 has access to it?
- How will that information be protected?
- Who will establish, control, and review these practices?

BIOMETRIC RDT&E CAPABILITIES

To evaluate potential RDT&E capabilities of an Army biometrics center, it is helpful to examine the role played by the National Biometric Test Center (NBTC) and the challenges found in testing biometrics. The U.S. government runs the NBTC at San Jose State University in California. James L. Wayman directs the NBTC, which is funded primarily through the NSA. NBTC's research interests are in application-specific testing of systems and in developing statistical methodologies for testing.[2]

[2] One of the reasons for NBTC's limited research agenda is that NSA is severely limited by law as to which data it can collect from U.S. citizens. See generally Executive Order 12333 (1981).

Commercial vendors and biometric consultants undertake evaluations of biometric devices. However, vendor testing alone fails to provide adequate information. From the perspective of motivation for testing, vendors and end-users have diverging goals. Vendors' reasons for testing include improving their devices and using the test results to sell their products. End-users seek testing results that will aid them in selecting a device that best fits their needs. Their focus is specific to their application and their enrollees.

Errors that affect biometric authentication devices potentially come from four different sources: variations in the biometric pattern, the presentation of the biometric to the sensor, the sensor, and the transmission process (including noise introduced by compression and expansion). Each of these factors is strongly tied to a specific application. One test environment cannot predict error rates for all applications. Hence, results from laboratory testing (vendor or otherwise) are highly dependent on the testing scenario population and are not necessarily a useful predictor of errors in real-world uses that differ from the testing scenario.[3]

Three important types of testing include algorithm verification, operational testing, and scenario evaluation:

- *Algorithm verification* occurs when testers evaluate algorithms used by a single device employing a database of "standard" samples. The results of this testing determine which algorithms are "good" and which are "poor." Although these tests are useful and repeatable, the results do not show real-life performance under real field conditions with real enrollee populations.
- *Operational testing* is typically used to evaluate pilot programs. It helps determine how the system will perform as a whole based on a specific application environment and the target population.
- *Scenario evaluation* is used to test the performance of multiple biometric systems in a modeled real-world application of interest to evaluate and compare performance across biometric devices. All devices are tested in the same environment on the

[3] Vendor or scientific laboratory testing generally presents only one scenario of biometric application: overt, cooperative, habituated, supervised, standard, closed, and private. See Appendix A.

> same population. This method allows for comparison of devices of different types. Scenario evaluation helps an end user decide which biometric device will work best for the end user's needs.[4]

What complicates testing is the fact that samples from thousands to millions of people are needed to test the distinctiveness of a biometric. Testing on these large sample sizes enables researchers to draw conclusions about uniqueness that are statistically significant. Biometrics also "age" or change over time. To acquire samples over any amount of time (from weeks to months or even longer) in any number of contexts from this number of people would be close to impossible, and to do this same testing for the many variables in each type of application would be even more difficult and probably too costly.

James Wayman (1999c) has summarized the three major difficulties in testing biometric devices and systems: "the dependence of measured error rates on the application classification, the need for a large test population that adequately models the target population, and the necessity for a time delay between enrollment and testing." Operational (e.g., field testing or pilot testing) and scenario evaluations, while expensive, are the only reasonable methods to test a system fully and reliably for deployment. Additionally, laboratory testing can be used to evaluate algorithms and as an initial pass/fail test for a biometric device to pass minimum standards before it is tested further either operationally or in a scenario evaluation.

An Army RDT&E center may also undertake further development of mathematical and statistical methods for test design and evaluation of biometric systems. It could also help develop standards or best practices for template collection, compression, and storage. An RDT&E center could be a source of advice on biometric systems for agencies inside and outside the Army, providing help to develop the educational roll-out piece of another agency's biometric program.

A CENTER FOR BIOMETRIC RDT&E SEEMS FEASIBLE

If the Army decides to pursue biometric technologies, it will likely want to establish a biometric RDT&E center to coordinate various

[4] Appendix A also discusses several other types of testing.

biometric activities, evaluate potential technologies, and adapt them to Army needs. As in other such labs, some work might be conducted in-house, but other functions would be contracted to other centers. Because the other armed services are also interested in the potential of biometrics, there may be calls for joining forces in a DoD-wide biometric RDT&E center. Similarly, other federal and state agencies working on biometrics might welcome the Army's help in creating a national RDT&E center that would serve broader governmental interests. For example, federal law enforcement agencies might eventually be interested in Army biometric data for use in criminal investigations. Furthermore, many federal agencies with whom the Army exchanges data might want to ensure that biometric data are standardized and systems are interoperable. In addition to test and evaluation functions, a larger center would presumably coordinate activities of the various members, ensure that technological developments and test results are shared, and even determine where future research efforts should be focused.

Whether the Army should seek the role of executive agent for a national biometric RDT&E center depends on the importance biometrics are expected to have in the Army. For example, if the success of the digitized Army depends on biometric technologies to protect battlefield intelligence nodes, then biometrics will be a high priority for the Army. If biometrics are one of many possible solutions to this problem, then perhaps the Army might want to retain more flexibility by pursuing biometrics within its own RDT&E structure or within a broader DoD structure.

AN ARMY OR DoD REPOSITORY FOR BIOMETRIC DATA ALSO SEEMS FEASIBLE

Based on our preliminary research, we believe an Army or DoD centralized repository for biometric data is feasible but not necessarily critical to the success of an RDT&E center. However, the feasibility ultimately depends on the purpose of the repository. This section details potential purposes for a repository and identifies the benefits and challenges associated with these purposes.

At a minimum, a central repository could be used to store templates collected for biometric programs. A central repository could play many useful roles. For example, if local authentication files are corrupted or erased, the central repository would have continuity of operations files or backup files that could be used. Furthermore, Army personnel move frequently and on short notice, so it might be useful to have a central repository for templates that could easily be transferred between facilities, much as security clearances are. However, given the ease of regenerating a template, the administrative difficulties of identifying the right template file, and concerns that old templates might not match the current individual (for biometrics that make adjustments with each use), it seems unlikely that the Army would rely solely on the repository to replace locally maintained templates.

Another reason to store templates is to support quality control and research at the biometric RDT&E center. Access to large numbers of biometric templates would help researchers test algorithms. However, templates would not be helpful in testing integrated systems because they would not provide such variables as user-sensor interactions and liveliness tests that are critical to the performance results of biometric systems.[5] Because template data can be transferred electronically, some might contend that no overwhelming need exists to co-locate the repository with an RDT&E center. The template data could be stored anywhere and simply accessed with a computer by those authorized to do so.

Finally, the Army may have legitimate reasons to store templates in a central repository. First, co-location with the RDT&E center could reduce risks associated with interception of biometric data. Second, at some point the Army could perform identification searches on the entire database of templates or on subsets of the database. This type of searching is likely to become much more feasible with advances in biometric technologies and computing power (see Appendix C, FBI Experience). Strengthened identification capabilities would allow biometrics to be used without accompanying cards or passwords, which would provide greater convenience to the biometric user.

[5] Liveliness tests are used in biometric applications to ensure that a person does not simply make a copy of your biometric, such as a Xerox of a fingerprint or a photograph of your face, and use this in the biometric sensor.

Concerns About a Centralized Repository

Security concerns about a centralized repository of biometric data are related to the vulnerability of that data as they are transmitted from the biometric reader to the repository and back again. The central repository might represent an attractive "honey pot"—attracting threats from hostile security services, hackers, and others seeking to compromise the integrity and security of network-accessible information. These vulnerabilities are not so different from those for passwords, PINs, or SSNs. Some would argue, however, that this vulnerability reduces the value of using biometrics, at least for remote verification applications. These transmission vulnerabilities can also be an argument for co-location of a test facility and repository, if they have an internal, highly protected network to safeguard the transfer of data.

A central biometric repository will also raise privacy concerns, depending on the purpose of the repository. Individuals will likely be more suspicious of a repository that only collects data than of one that verifies biometrics remotely. Given current computer power, widespread real-time matching against an entire DoD-wide repository seems unlikely to be feasible. However, as noted above, remote verification will raise privacy concerns, because the data are vulnerable to capture and tampering when they are in transmission. For some, storing all biometric data at one location can be more worrisome than having it dispersed because concentration of data lends credence to theories that the data will be used for tracking or purposes other than the ones advertised. A central repository would make sharing data with other organizations easier. At the same time, centralized control can make it easier to protect the data from misuse or function creep because only one staff member must be educated as to the rules for data protection and data-sharing.

Analysis

The issues raised here with respect to an Army biometric data repository are not likely to be significantly different if the repository served all of DoD. Considerable data-sharing exists at present and large amounts of personal data are consolidated in databases managed by the Defense Manpower Data Center, for example. Moreover, the military's emphasis on joint operations and other interservice endeavors suggests that the Pentagon might want to take a DoD-wide approach to biometric applications to ensure standardization and interoperability, rather than having each service field its own biometric systems.

Concerns about a repository are also likely to depend on whose biometric templates are included. Keeping service members' biometric data could account for millions of records, depending on the purpose of the program and the problem being tackled. As the circle is expanded to include Department of the Army or DoD civilian employees, contractors, retirees, dependents, and foreign nationals, more concerns will likely be raised about protection of privacy and purposes of the data and centralized repository. To the extent it is concerned about ensuring data privacy, the Army, by operating a repository serving its own or DoD's needs, could take the lead in influencing data protection and related policies.

If the Army takes the lead on a DoD repository, its role could expand to become that of the head of a national biometrics repository, serving all of the federal government, for example. It is not clear what the purpose of a national repository would be, and, thus, it is difficult to evaluate the feasibility of establishing such a national center and the value to the Army of running it.

A NATIONAL BIOMETRICS DATA REPOSITORY RAISES SERIOUS FEASIBILITY ISSUES

Based on our research and analysis to date, a national biometric data repository raises serious feasibility issues. While a national repository could serve useful purposes, such a center may provoke concerns for privacy protection.

Among the useful purposes it could serve, a national biometrics repository could provide for efficiency and interoperability. If other federal agencies using biometrics also find it necessary to store templates, and a large repository of data from military personnel already exists, then other federal agencies might want to build on the Army's expertise and use the Army's repository for template storage—perhaps on a fee-for-service basis. Congress might also proceed further down the path of data-sharing for law enforcement purposes and take steps to ensure that biometrics collected for military, federal employment, and licensing requirements are made available to law enforcement authorities under certain conditions**.** The FBI appears to be considering a move in this direction when automation of fingerprints makes this possible. Such data-sharing might also be envisioned as a method to reduce fraud in social service programs, in much the same way as states have used biometrics to identify double-dippers. Perhaps a national biometrics data repository would be made available to federal and state social service agencies to ensure that only qualified individuals are receiving benefits.

Opponents of such a national biometrics repository will draw comparisons to the ubiquitous use of SSNs as an identification number despite the original assurances by the government that the SSN was not to be used for other purposes. As the population providing biometrics for the repository grows, so too will objections increase. Servicemembers, who already sacrifice many of their freedoms to serve in the military, are likely to be compliant. Similarly, the large circle of people with ties to DoD will also be expected to generally accept the need for a centralized repository. However, expanding the circle of participants to include other federal employees, social service recipients, and people who have had background checks will increase the number of people likely to raise concerns.

While the Army might like to have access to others' biometric data, such as fingerprints, it is not clear that its need is sufficient to take on the burden of running a national repository. The Army can obtain this information in many ways, such as data-sharing arrangements with other federal and state agencies. For example, if law enforcement purposes are the primary motivation, it would seem that the FBI should administer the national repository. Similarly, if fraud prevention in social service programs is the primary aim, perhaps the Department of Health and Human Services should take the lead.

With a national repository, not only would the possibilities for data-sharing be greater but pressure from various agencies to gain access to others' data would also increase if the center resided in one location, even if in separate databases. Furthermore, it seems likely that the agency in charge of managing the biometric repository would have access to much more data than any one agency in the federal government currently has.