Chapter Four

WHAT STEPS CAN THE ARMY TAKE TO ADDRESS THESE CONCERNS?

Given the three major sociocultural concerns associated with the Army's use of biometrics, namely protecting informational privacy, safeguarding physical privacy, and addressing religious objections, this chapter focuses on how the Army can most effectively address these concerns. Because biometrics are similar in many ways to more traditional identifiers, such as photographs, the Army can look to existing laws, regulations, and precedents to address the main sociocultural concerns. This body of law suggests that the Army has a solid framework in place to address sociocultural concerns.

However, in light of the novelty of the technology and the heightened interest among citizens in informational privacy, it may be prudent for the Army to address concerns about biometrics within the context of a broader approach. By doing so, the Army can reassure its community and the American public that it takes the use of biometrics and protection of privacy and religious freedoms seriously, its biometrics program is well-thought-out, it has taken reasonable precautions to protect personal data, and it has made choices about the technologies being used and the structure of the program with consideration for their effect on individuals.

In this chapter, we begin by discussing legal precedents and related policies and procedures the Army might apply to address the specific sociocultural concerns discussed in Chapter Three.[1] We conclude by

[1] Readers interested in a more detailed legal assessment should refer to Appendix C.

discussing what a comprehensive approach to managing these concerns ought to entail.

PRIVACY ACT OF 1974: A BASELINE FOR ADDRESSING SOME SOCIOCULTURAL CONCERNS

Personal information in the hands of the Army is not a new issue. Accordingly, many of the sociocultural concerns raised by the use of biometrics can be addressed through Army policies and procedures established to carry out the requirements of the Privacy Act of 1974. The Privacy Act regulates the collection, maintenance, use, and dissemination of personal information by federal government agencies, including DoD and the Army. Although the Act does not specifically mention biometrics, analysis suggests that many Army biometric programs would fall under this Act, in particular those biometric applications involving "a system of records."[2]

The Privacy Act gives certain rights to the individual who provides personal information and places certain responsibilities on the agency collecting the personal information. While the Privacy Act addresses informational privacy concerns, it does not address physical privacy and religious freedom concerns.

The Privacy Act's basic provisions, reflected in both the DoD Privacy Program and the Army Privacy Program,[3] include the following:

- Restricting federal agencies from disclosure of personally identifiable records maintained by the agencies.
- Requiring federal agencies to maintain records with accuracy and diligence.

---

[2]The Privacy Act applies to a "record" that is "contained in a system of records." While the Act's definition of record includes any "other identifying particular assigned to the individual such as a finger or voice print or a photograph" (see 5 U.S.C. § 552a(a)(4)), not all biometric programs are necessarily contained in a system of records. For example, the Fort Sill test of a biometrically protected smart card (see Appendix B) was not contained in a system of records because the biometric was stored only on the card and not in any central database. The Fort Sill test is an example of a biometric being used to enhance privacy.

[3]Unless otherwise indicated, the Privacy Act provisions discussed here apply to DoD and the Army.

- Granting individuals increased rights (1) to gain access to records maintained on them by federal agencies and (2) to amend their records provided they show that the records are not accurate, relevant, timely, or complete.
- Requiring federal agencies to establish administrative, technical, and policy safeguards to protect security of records.[4]

To ensure compliance with the Act, DoD and the Army have established several institutional assets to help oversee policies and procedures related to privacy. For example, DoD has a Defense Privacy Board and supporting staff in the Defense Privacy Office.[5]

The Act requires those agencies establishing systems of records to publish in the *Federal Register* information about the systems of records in their charge, give individual notice of the uses to which the data will be put, and safeguard data. The Army now has 249 systems of records for which notice must be published. These systems range from "Official Personnel Folders and General Personnel Files" to "Individual Health" to "Carpool Information/Registration System."[6] As Army use of biometrics will likely lead to the establishment of new systems of records and revisions to old systems, the Army must comply with this Privacy Act Systems of Records Notice requirement.

The Act's requirement that individuals be given notice addresses many of the concerns raised in Chapter Three. The notice must state the authority sanctioning the solicitation of the information, the purpose for which the information is intended, the routine uses that may be made of the information, whether the data collection effort is voluntary or mandatory, and the implications to the data subject of failing to provide the requested information.[7]

---

[4]See, e.g., Cate (1997, p. 77).

[5]The Army can draw on the many existing institutional assets who have extensive experience in Privacy Act matters. These assets include the Defense Privacy Board, the Assistant Secretary of Defense (Comptroller), the Defense Privacy Office, the DoD General Counsel, the Army Assistant Chief of Staff for Information Management, the Army General Counsel, the Army Judge Advocate General, the Deputy Chief of Staff for Personnel (DCSPERS), OMB, and many others.

[6]See Department of the Army (2000).

[7]See 5 U.S.C. § 552a(e)(3)(A)-(D). The authority may be granted by statute or executive order of the President. See 5 U.S.C. § 552a(e)(3)(A).

Although the Act prohibits a federal agency from "disclos[ing] any record without the consent of the individual to whom the record pertains," it provides for certain disclosure exceptions listed below.[8] These twelve exceptions to the "No Disclosure Without Consent" Rule are:

- the "Intra-Agency Need to Know" Exception,
- the "Required Freedom of Information Act (FOIA) Disclosure" Exception,
- the "Routine Use" Exception,
- the "Bureau of the Census" Exception,
- the "Statistical Research" Exception,
- the "National Archives" Exception,
- the "Law Enforcement Request" Exception,
- the "Individual Health or Safety" Exception,
- the "Congressional" Exception,
- the "General Accounting Office" Exception,
- the "Judicial" Exception, and,
- the "Debt Collection Act" Exception.

Some privacy advocates contend that the routine use exception has been used by federal agencies to justify almost any use of the data (Cate, 1997, p. 78, footnote omitted). For example, the Army has a so-called "law enforcement blanket routine use," which applies to every record system maintained by the Army, unless specifically stated otherwise. The law enforcement blanket routine use allows the Army to share routinely any record indicating a potential violation of the law with the appropriate federal, state, local, or foreign agency charged with investigating the matter.[9] Similarly, the Army

[8]See 5 U.S.C. § 552a(b).

[9]See, e.g., OMB Guidelines, 40 Fed. Reg. at 28,955 (proper routine use is "transfer by a law enforcement agency of protective intelligence information to the Secret Service"). See also 28 U.S.C. § 534 (authorizing Attorney General to exchange criminal records

routinely discloses any records indicating a possible violation of law, regardless of the purpose for collection, to law enforcement agencies for purposes of investigation and prosecution.[10] On the other hand, the Army can exempt certain programs from this "law enforcement blanket routine use." For example, it does not apply to the "Armed Forces Repository of Specimen Samples for the Identification of Remains" System of Records, which includes "specimen collections from which a DNA typing can be obtained."[11]

The Army does not necessarily have the final say over how its data will be used or shared. Congress can always mandate additional new "routine uses" for data. For example, Congress has mandated the establishment of a federal "Parent Locator Service" and requires federal agencies to comply with requests from the Secretary of Health and Human Services for addresses and places of employment of absent parents.[12]

As noted above, the Privacy Act also requires the federal agency to put in place appropriate safeguards to protect information in its databases.[13] Both the agency and the employee responsible for any breach can be found legally liable for a Privacy Act violation, including civil liability for the agency and criminal liability for the individual.

In *Whalen v. Roe*, the Supreme Court directly addressed informational privacy concerns.[14] *Whalen* involved the constitutional question of whether the State of New York could record and store, in

---

with "authorized officials of the Federal Government, the States, cities, and penal and other institutions").

[10]See OMB Guidelines, 40 Fed. Reg. at 28,953; see also 28 U.S.C. § 535(b) (1994) (requiring agencies of the executive branch to expeditiously report "[a]ny information, allegation, or complaint" relating to crimes involving government officers and employees to the U.S. Attorney General).

[11]See 63 Fed. Reg. 10205, March 2, 1998. See also Armed Forces (2000).

[12]42 U.S.C. § 653.

[13]The Privacy Act requires the data collector to "establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records." Similarly, the Act requires the data collector "to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained."

[14]*Whalen v. Roe*, 429 U.S. 589 (1977).

a state-run, centralized, computerized database, the names and addresses of anyone who had obtained certain drugs pursuant to a doctor's prescription. The Supreme Court held that the New York database containing massive amounts of sensitive medical information passed constitutional muster. In particular, the Court cited New York's need for the database as part of the state's war against drugs and noted that the New York statute and its related implementation, including extensive database protections, showed "a proper concern with, and protection of, the individual's interest in privacy." The Court, however, reserved for another day consideration of legal questions that could arise from unauthorized disclosures of information from a government database "by a system that did not contain comparable security provisions."[15]

Concerns about misuse of data and the possibilities of identity theft could be addressed in part by Army procedures already established to respond to Privacy Act requirements. Specifically, the Privacy Act requires the Army to use appropriate data safeguards and carries the threat of civil and criminal sanctions if these requirements are not carried out.

In summary, from the perspective of those concerned about the Army's biometrics program and center, the Privacy Act addresses concerns related to the purpose for which the data will be collected, the notification of individuals that their personal information is needed, and how the information will be used and shared. In addition, the Privacy Act requires government agencies and officials to secure their database.

The Privacy Act permits many exceptions, and the Army could make many routine-use exceptions for biometric identification information. Although additional uses of the data beyond the original purpose for which it was collected must be published in the *Federal Register* and shown to be compatible with the original use, this is not a serious obstacle to the sharing of data. Thus, it leaves the individual without much firm protection against function creep.

The Army should strive to address function creep concerns through laws, regulations, and policies designed to ensure that biometric data

---

[15] *Whalen v. Roe*, 429 U.S. at 605–606.

are used only for purposes explicitly stated and that even marginal changes are reviewed by appropriate policymakers or senior leadership. Protection against function creep will help ensure that the data are not used for tracking unless that is a specifically stated goal.

OTHER MILITARY POLICIES ADDRESS SPECIFIC SOCIOCULTURAL CONCERNS

Beyond the issues raised by the Privacy Act, the Army can rely on other military policies and procedures to further address religious concerns. Precedents found in the case law address intrusiveness concerns.

Religious Objections

The military is no stranger to addressing the religious concerns of its members. The Army's use of biometrics is likely to be met with objection on religious grounds by a small number of personnel. The Army has an extensive, established policy in place to accommodate religious practices.[16] The Army approves requests for accommodation of religious practices unless the accommodation will have an adverse impact on "military necessity," which consists of unit and individual readiness, unit cohesion, morale, discipline, safety, and health. As the Army's primary advisor on matters pertaining to religious accommodation, the Army Chief of Chaplains is an important institutional asset on whom the Army leadership may call for guidance in determining how religious objections to biometric applications should be handled. As the official charged with establishing the Army's policy on the accommodation of religious practices, the Deputy Chief of Staff for Personnel (DCSPERS) will also have a key role to play.

Physical Privacy

The federal courts have yet to decide any cases involving an individual's refusal to participate in a biometric program mandated by the federal government. However, the Army can draw parallels to legal

[16]See Army Regulation (600-20, 1999).

challenges brought to fingerprinting in a noncriminal context—when an individual must provide a copy of his fingerprints for employment purposes, for example. The courts have generally upheld federal, state, and municipal requirements for fingerprinting as a condition of employment and licensing, provided the government has a rational basis for the requirement. For example, a union representing some 5,170 utility workers employed at nuclear power plants challenged as unconstitutional that part of a federal statute requiring these workers to be fingerprinted. The federal court disagreed with the union and upheld the fingerprint requirements. The court found that the U.S. government had a rational basis for requiring fingerprinting, namely concern over security at nuclear power plants.

What will happen if the Army wants a specific biometric from a person in a criminal justice context—because it suspects the person of a crime, for example? The Fourth Amendment to the U.S. Constitution governs searches and seizures conducted by government agents. As the amendment makes clear, the Constitution does not forbid all searches and seizures, only "unreasonable" ones. The Supreme Court defines a search as an invasion of a person's reasonable expectations of privacy.[17] To evaluate whether providing a biometric identifier in a criminal justice context constitutes a search, the judiciary focuses on two factors. First, the Court examines the nature of the intrusion.[18] Actual physical intrusions into the body, such as blood-drawing, breathalyzer testing, and urine analysis, can constitute Fourth Amendment searches. Second, the Court examines the scope of the intrusiveness, paying close attention to the "host of private medical facts" revealed during the search.

In cases where provision of a biometric identifier might be found to constitute a search (as in the hypothetical case of a physically intrusive DNA-based biometric that would reveal extensive medical facts), the ultimate measure of the constitutionality of a governmental search is "reasonableness."[19] To make this determination, a court must balance the "intrusion on the individual's Fourth Amendment interests against its promotion of legitimate governmental

---

[17]See, e.g., *Katz v. United States*, 389 U.S. 347, 360-62 (1967) (Harlan, concurring).

[18]See *Skinner v. Railway Labor Executives' Ass'n*, 489 U.S. 602, 616 (1989).

[19]*Vernonia Sch. Dist 47J v. Acton*, 515 U.S. 646, 652 (1995).

interests."[20] For a search to be reasonable, in the criminal justice context, the Army must generally show probable cause to believe that the person or place searched is implicated in the crime.

RESPONDING TO SOCIOCULTURAL CONCERNS WITHIN A BROADER APPROACH IS CRITICAL

Our legal assessment has raised no significant obstacles to the Army's establishment of a biometrics program or center in the United States. In fact, many military regulations and procedures are already in place to help address the concerns that might be raised by a biometrics program and center. By its implementation of the Privacy Act and its own policies on religious accommodation, the Army addresses two of the three major concerns identified with biometrics: concerns about privacy, including fears of government tracking and the collection of additional information or distribution of personal information, and infringement on religious freedoms. Concerns about misuse of data and identity theft are addressed, though less directly, through provisions in the Act related to the obligations of the data collector to protect security. Concerns about physical intrusiveness do not seem to have legal standing for current biometrics although this may change if medical information becomes part of the personal information revealed in a biometric.

These findings do not mean that the Army can avoid responding to perceptions about biometrics. Despite its legal feasibility, biometrics use by the Army could still be overturned by concern in the military or in the larger society about the program. Given these concerns, it is critical for the Army to take additional steps to improve perceptions of its biometrics program. Such an approach includes four steps.

- Thoroughly explain why biometrics are the best solution to a particular problem.
- Structure a program and select technologies to minimize effects on privacy.
- Educate the Army community and the public about the purpose and structure of the Army's program.

---

[20] *Id.* (quoting *Skinner*, 489 U.S. at 619) (internal quotation marks omitted).

- Assign responsibility within the Army for guiding these steps.

Thoroughly Explain Why Biometrics Are the Best Solution to a Particular Problem

The Army must be prepared to justify its program by defining a compelling problem and explaining why biometrics (or a specific biometric application) are the preferred solution. The justification should include a detailed description of the problem it intends to address with biometrics. It should describe and evaluate a range of alternative solutions, including biometrics. The criteria for evaluation should be clearly stated. This justification is the basis on which individuals and society will decide whether their concerns about biometrics should be secondary to the common good. Policymakers will base their judgments on these arguments as well.

Many individuals, particularly those in the military, have a high regard for the need to protect information and facilities, and those arguments, if backed by sound analysis, will carry considerable weight with soldiers, civilians, contractors, and families. To many of them, a well-thought-out biometrics program will be a logical improvement to existing security procedures. The threat posed by weaknesses in the current programs and the importance of biometrics to solving this problem will be the basis of decisions made by policymakers and legal counsel with regard to the structure of the program, the importance of enforcing compliance, and the extent of accommodations for legitimate individual concerns.

There are no laws, regulations, or specific procedures in the Army or DoD to ensure that the Army defines a compelling problem and that biometrics are the best solution. Were the Army to be the sole proponent of biometrics, this analysis would come from within as part of the argument for funding a biometrics program. Given pressures from outside DoD to move these activities forward, the problem analysis could be neglected—an oversight that could prove destructive as the program becomes more concrete.[21]

---

[21]Moreover, fast-paced commercial developments with the emerging technology could also push the Army in uncomfortable or unexpected ways. For example, if, in the near future, major computer manufacturers, software developers, and Internet

The justification will define the purpose of the biometric program. If the purpose is clearly related to a problem and is narrowly defined, individuals are likely to be less concerned about giving up information (and privacy) than if the purpose is more broad-based. The importance of ensuring a clearly defined purpose is supported by the Supreme Court's reasoning in its leading case on informational privacy, *Whalen v. Roe*. In *Whalen*, the Court found that the New York statute mandating a computerized database addressed a compelling problem and that the state agency had taken comprehensive measures to protect the database from unwarranted intrusions.

Defining the purpose also provides a context for determining the data to be collected. If the purpose of the program is to verify the identity of individuals for facility or information access control, there would be no need to collect information other than the biometric. If the Army wants to include other data, such as levels of access or a person's name, it should make the reasons for this clear to the participants and the general public. Because the biometrics currently in use have not been shown to contain medical information, the answer to the question, "What data is provided by the biometric?" would seem to be "None, other than the physical characteristics associated with an individual's biometric."

Structure a Program and Select Technologies to Minimize the Effects on Privacy

Three issues must be addressed in making decisions about how to design a biometrics program and select technologies:

- Policies about sharing data.
- Privacy enhancing solutions.
- Data repository choices.

---

providers embrace biometrics for computer and network access, this commercial development might influence Army commanders to demand the technology for immediate deployment. Instead of having in place a uniform policy for biometrics and their use, the Army might approach biometric use piecemeal, without any comprehensive planning in place. Although experimentation is generally welcome, the Army should have a biometric policy in place that will, at a minimum, address sociocultural concerns.

Policies about sharing data determine who will have access to the biometric database and for what purposes. From a privacy perspective, policies should be as restrictive as possible to limit the possibilities of function creep and the development of tracking capability. Even if the database contains only biometric information, concerns will arise about the extent to which the information will be shared to serve other purposes and whether and how participants will be notified of these additional purposes. For some purposes, however, other data, such as financial or medical information, might be tied or linked to the biometric.

As noted earlier, decisions the Army makes related to sharing of biometric identification information will be viewed as an important indicator of how seriously the Army takes its privacy protection responsibilities. As the Army considers which exceptions might be requested with respect to biometrics, it might benefit from study of the ongoing FBI experience involving the bureau's searchable criminal and civil fingerprint databases. In particular, the Army will be interested in the conclusion of the FBI's Office of General Counsel that the FBI's use for criminal justice purposes of fingerprint records obtained from service members and federal employees among others is legally unobjectionable. (See Appendix C, FBI Experience.) However, such a use will be a matter of concern to those who would like to limit sharing of personal information between military and law enforcement organizations.

Establishing a board or committee to assess biometric data policies, particularly with respect to data sharing for medical or biometrics-related research could also show a good faith effort to protect individuals' privacy. Policies regarding the destruction of biometric data will also affect privacy perceptions. Holding biometric data after a person loses access to a particular system or facility or leaves the service will exacerbate perceptions that the Army is collecting these data for purposes other than those stated.

Privacy enhancing solutions should be one of the criteria the Army uses in choosing biometric technologies. The design of data authentication and storage procedures will affect privacy perceptions. In choosing the biometric technology and structuring its program, the Army can address some of the privacy concerns raised about biometrics. Today, verification applications are thought to enhance

privacy more than those using biometrics for identification. At a minimum, biometrics should add a level of protection and, in some cases, are likely to enhance privacy, such as applications using smart cards protected by biometrics (as in the Fort Sill pilot program).

Using less distinctive or robust biometrics for appropriate applications, such as verifying access by a limited group of authorized users, is another way to limit function creep and tracking capabilities. The INS's INSPASS program used at selected airports as an alternative to waiting in the immigration line is an example of this. Hand geometry is used because the relatively few users are prescreened. Yet hand geometry is probably not distinctive enough to use in an identification application.

Another way to address privacy concerns is to use biometrics with multiple options or "availability," such as fingers, and to use different biometrics for different programs. This would make it more difficult to engage in tracking and might limit pressure for function creep by reducing the number of templates in any particular technology.

Although use of multiple biometrics for different purposes in the Army might raise concerns that it is building a tracking database using many different features, some privacy experts would take a different view. Some have proposed that use of multiple biometrics protects an individual by ensuring compartmentation.[22] For example, a fingerprint used to gain access to the lab cannot be associated with a facial image used to get into the base exchange. All the biometric can do is ensure that the fingerprint or the image matches templates authorizing access to those facilities. The system does not need to know to whom these images belong or how to connect the purchasing patterns of the scientist with the hours he is in the lab.

Using multiple biometrics depending on the program needs and minimizing use of central repositories will not only help alleviate concerns about tracking, but it will also minimize demands on the Army to share the data, connect databases, and contribute to function creep. Technical obstacles to connecting data as well as policy and procedural practices that limit the purpose and uses of the data will bolster the Army's position that it is serious about the privacy of

[22]See, e.g., Wayman (1998).

biometric data. Commitments to avoid biometrics that contain medical information, such as DNA, even if they become commercially viable, might be another policy the Army would want to adopt.

The various experts interviewed repeatedly stressed that careful planning and attention to detail are important components of a successful biometrics program. Detailed planning includes such steps as addressing the accessibility of biometric systems for persons with disabilities, determining whether particular individuals in a facility will object to certain biometric technologies or would be unable to enroll, and realizing that military affiliated personnel and the public at large will have limited tolerance for large-scale biometric programs that do not work or work only for a subset of those enrolled. Planning should not be limited to the performance of the technology but must consider the range of people using the biometric, ensuring that physically impaired people can use the device.

Data repository choices also affect perceptions of privacy and security. One way to enhance security is to use biometrics that do not require templates to be sent to a central repository for matching or to decentralize storage and matching altogether, using a smart card. Systems that send a template to a central repository for comparison run the same risks as other information transmitted "over the wires." That is, the information transmitted can be intercepted at a number of points, resulting in the theft of either the biometric template or the authorization to accept the stolen or blocked biometric, depending on the purpose of the saboteur. Encryption, use of sequence numbers, time stamps, and other electronic data protection methods can help safeguard these transmissions, but they are not as inherently secure as systems that do not transfer the data. On the other hand, programs protecting access at one location, be it desktop or building or base, can design systems in which all the data is held locally.

Educate the Army Community and the Public About the Purpose and Structure of the Program

Openness and education about the program are two ways to address concerns that the biometric data contain additional information or that the data will be used inappropriately. Whether the program is large or small, personnel will need to be informed of the program

and educated about it. The Army's education campaign should address the following questions:

- 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?

Although it is possible to undertake smaller programs with limited publicity, the establishment of a national biometric center would require considerable public education on these topics. Nearly all the program experts, lawyers, and ethicists interviewed for this project noted the importance of an education campaign to build support for any personal information collection program, particularly when a large population will be included. The Army's experience with biometrics includes small- as well as large-scale programs, such as those at Fort Sill or the military's DNA Human Remains Identification program. A critical component of their success has been educating the personnel involved about the purpose and limits of the program, as well as control of the data records.

Assigning Responsibility in the Army for Guiding These Steps

The Army has many decisions to make as it develops a larger biometrics program and, potentially, a biometrics data repository and test center. The issue of who guides these decisions initially and in the future is critical to the Army's ability to sustain its biometrics program. Who reviews requests for access to biometric data—be it for medical research or law enforcement purposes? Who ensures that the biometrics program is responsive to privacy concerns?

The Army's choices in implementing its biometrics program, and particularly when establishing a biometrics repository, should be consistent with the need to protect privacy and with its public commitments to do so. Decisions must be made about where to use biometrics, who must be included, and what data will be linked to the biometrics.