Chapter Three

WHAT CONCERNS DO BIOMETRICS RAISE AND HOW DO THEY DIFFER FROM CONCERNS ABOUT OTHER IDENTIFICATION METHODS?

Any biometrics program must be prepared to deal with individuals who cannot or will not participate in the program. Some people, through no fault of their own, cannot provide the chosen biometric because they have unmeasurable fingerprints or eyes, for example. Thus, all biometric systems have a small number of people who simply cannot be enrolled.

Others, however, deliberately choose not to participate in biometric programs because of their individual beliefs. While these individuals constitute a relatively small minority, they are the most likely contingent to voice their concerns. Their criticism will probably not cause a biometric program to collapse or render it ineffective. However, such criticism could inhibit a biometric program's development, implementation, and support. Thus, the Army must bear in mind that biometric technology is not without its critics,[1] and it must take into account current and potential sociological concerns.

In this chapter, we answer the question of what sociocultural concerns biometrics raise and whether these concerns differ from those related to other identification methods. In response to the first part of the question, we identify and briefly discuss three key sociocultural concerns: informational privacy, physical privacy, and reli-

[1] See, e.g., Garfinkel (2000), discussing privacy concerns of new technologies including biometrics, and Woodward (1997a), surveying the privacy enhancing and privacy threatening aspects of biometrics.

gious objections. With regard to the second part of the question, we find that while similarities exist among the concerns, differences exist between biometrics and other identification methods.[2]

Background. In the United States, the freedom of the individual is perceived to be closely related to his ability to operate somewhat autonomously and anonymously in the eyes of the state as well as other organizations. For example, we cast secret ballots; we have certain legal rights to decisional, informational, and physical privacy; and we have placed constraints on the sharing of personal information about us within the federal government. Although constraints on the sharing of information about us by other organizations are more limited, we, as a society, are grappling with how best to respond to the capabilities information technology affords.

Biometric applications have the potential to further reduce anonymity. In addition, as with any technological innovation, some people will find certain aspects of biometrics discomforting or unacceptable for a variety of sociocultural reasons. Some of these reasons may be recognized by our societal ethics and laws, such as those protecting religious freedom and privacy rights. However, as a society, we acknowledge, and the laws reflect, an expectation that in some cases the needs of society will override individual objections to participating in an Army biometrics program or any other government-mandated biometrics program. If the discomfort with such a program seems to arise from unfamiliarity with a new technology, as opposed to deep-seated moral or religious objections, the decision about whether to force compliance with the new program must weigh the importance of the societal need for the new program against societal concerns for individual rights. In a type of utilitarian calculus, the law also recognizes the necessity to balance the needs of the whole against the rights of the individual.

A review of past and current biometric programs suggests that the use of biometrics in the United States evokes several sociocultural concerns. These concerns may be based on a variety of factors, including fears about the centralization of biometric identification information and the potential for misuse of these data, concerns

[2]Biometric programs provided important insights to this part of our research. Descriptions of some may be found in Appendix B.

about the physical intrusiveness of the technology, and religious objections to the technology's use.[3]

These issues will more fully evolve over time and may change significantly as biometrics are introduced more broadly through private sector and public sector applications. It seems likely that as biometrics become more pervasive, the research community will begin to determine whether these measures can reveal more about a person than only his identity. For example, knowing that certain medical disorders are associated with specific fingerprint abnormalities, researchers might actively investigate such questions as, can fingerprint template patterns be linked to behavioral characteristics, or predispositions to medical conditions? If these questions are answered affirmatively, biometrics might become not only an identifier, but also a source of information about an individual. Such a development would likely have a significant impact on how biometrics are perceived and managed in the United States and abroad.

KEY SOCIOCULTURAL CONCERNS

The key sociocultural concerns associated with biometrics fall into three main categories:

- Informational privacy.
- Physical privacy.
- Religious objections.

Informational Privacy

The most significant informational privacy concerns relate to the threat of function creep and the tracking capabilities of biometrics. These concerns are addressed below.

Function Creep. Function creep, or mission creep, is the process by which the original purpose for obtaining the information is widened

---

[3]See Appendix B, Program Reports, Citicorp Clip Card and Security Infrastructure and Columbia Presbyterian Hospital, for examples of privacy concerns raised during program implementation.

to include purposes other than the one originally stated. Function creep can occur with or without the knowledge or agreement of the person providing the data. Many privacy experts contend that function creep is inevitable.[4]

Depending on whom it affects and how it affects them, function creep may be seen as desirable or undesirable. For instance, using SSNs to search for a parent who is delinquent with child support payments may be seen as desirable. On the other hand, having a person's digitized state Department of Motor Vehicles (DMV) photograph sold to a commercial firm to create a national photo ID database might be considered unacceptable (Davies, 1994, pp. 61–62).[5]

Additional purposes can be useful and valuable to society, but ethical concerns arise when biometrics are used beyond their original purpose, without the informed and voluntary consent of the participants. These concerns include whether participants have the right to reassess their participation given the new purpose for the data, the implications of a decision not to cooperate in providing biometric data, and justification of the new purposes, given the program's original intent.

Tracking. The use of massive databases containing detailed personal information in both the public and private sectors has raised concerns about an individual's ability to maintain his or her anonymity (Garfinkel, 2000, pp. 1–36). Some people fear a "Big Brother" government able to track every individual. Tracking, which may be thought of as a particular type of function creep, refers to the ability to monitor in real time an individual's actions or to search databases

---

[4]For example, Simon G. Davies (1994), the Director of Privacy International, has explained:

> The history of identification systems throughout the world provides evidence of "function creep"—application to additional purposes not announced, or perhaps even intended, at the commencement of the scheme. . . . The existence of a relatively high-integrity scheme would create irresistible temptations to apply it widely, and interrelate many hitherto separate collections of personal information.

[5]In fact, South Carolina sold photographs of the state's drivers to Image Data LLC, a New Hampshire company.

that contain information about these actions. For example, if an individual must use a standard biometric for multiple governmental, business, and leisure transactions of everyday life, it becomes possible that each of these records could be linked through the standardized biometric. This link could allow an entity, such as the government, to compile a comprehensive profile of the individual's actions. This Big Brother concern has been expressed by privacy expert Roger Clarke (1994, p. 34):

> Any high-integrity identifier [like biometrics] represents a threat to civil liberties, because it represents the basis for a ubiquitous identification scheme, and such a scheme provides enormous power over the populace. All human behavior would become transparent to the state, and the scope for non-conformism and dissent would be muted to the point envisaged by the anti-Utopian novelists.

The possibility of clandestine capture of biometric data increases concerns about Big Brother. For example, facial recognition systems can track individuals without the individual's knowledge or permission. This alone raises ethical concerns. Moreover, the information from tracking can be combined with other personal data, acquired through biometrics or other means, to provide even more insight into an individual's private life.[6]

Misuse of Data. Misuse of personal information, including the stealing of identities (identity theft), has become more of a threat as information technology, including electronic commerce, has become ubiquitous. Used in certain ways, biometrics provide greater security because the biometric identifier is much harder to steal or counterfeit. As sociologist Amitai Etzioni (1999, p. 125, emphasis added) has explained:

> Reliable identifiers could replace the existing patchwork of passwords that are often forgotten, lost, or misappropriated. The same identifiers could be used to ensure that one's vote is not forged, that one's credit card is not misused, that one's checks are not cashed by

[6]Earlier this year, controversy surrounded the disclosure that law enforcement used facial recognition to surreptitiously surveil spectators at the Super Bowl in Tampa, Florida, in an effort to identify would-be criminals and terrorists. See, e.g., Woodward (2001), Piller et al. (2001), and Slevin (2001).

> others. . . . In short, reliable universal identifiers—*especially biometric ones*—could go a long way toward ensuring that people are secure in their identity, thereby allowing others to trust that they are who they claim to be.

On the other hand, where biometrics are authenticated remotely, that is, by transmission of data from a sensor to a centralized data repository, a hacker might be able to steal, copy, or reverse-engineer the biometric.[7] This misappropriation could also come about through insider misuse—e.g., the rogue employee. Without proper safeguards, files could be misappropriated and transactions could be performed using other people's identities.

Physical Privacy

The use of biometrics may raise physical privacy concerns. These concerns are threefold: the stigma associated with some biometrics, such as fingerprints; the possibility of actual harm to the participants by the technology itself; and the concern that the devices used to obtain or "read" the biometric may be unhygienic.

Stigmatization. Concerns about stigma vary tremendously in society. In the United States, some individuals and segments of society associate fingerprinting with law enforcement, acts of criminal behavior, and oppressive government (Garfinkel, 2000, pp. 43–44). However, among the voluntary private sector programs we reviewed that used fingerprints (see Appendix B), no program managers cited this stigma as a concern among participants. Stigmatization may be more of an issue for participants in mandatory programs, such as those the Army would implement, as well as biometric applications that have been implemented by state departments of social services. The program managers we spoke with, however, indicated that these objections were easily overcome through education about the protections that would be in place on using and safeguarding biometric data.[8]

---

[7]See Appendix B, Program Reports, Fort Sill Program, as an example of concerns over reverse-engineering fingerprints.

[8]The outreach and public education programs of the state social services departments generally focused on the benefits for social services clients by having a biometric

All service members and applicants for federal employment must provide fingerprints to the FBI as part of a background check. Hence, to this group, fingerprinting is nothing new. Based on our discussions with international privacy experts and program managers, it appears that fingerprinting is more of an issue in other nations and cultures, although several foreign biometric programs use fingerprints and report little concern about social stigma among their populations.

Actual Harm. Concerns about actual harm that could be caused by biometric technologies are primarily perceptual. Although the technology is in fact harmless, the perception of harm may cause users to obstruct the implementation of a program or be reluctant to participate in it. For example, we can imagine military pilots, whose careers depend on their eyesight, being greatly concerned about a biometrics program that requires them to look in close proximity at a device to have their retina scanned. Others may be concerned that a dismembered limb could be stolen and used to "fool" a system.

Hygiene. Objections to biometrics based on concerns about the cleanliness of sensors is another issue. Much as with concerns of the cleanliness of public restrooms, participants may feel uncomfortable placing their faces against a machine to have their retinas scanned after many others have done so or touching a hand-geometry scanner during flu and cold season. However, we know of no biometric application overturned for hygienic reasons.

The degree to which objections based on physical requirements might arise, if at all, are likely to be correlated with the biometric technology chosen, the size of the group using the biometric, and whether the sensor is shared by many (as with a hand-geometry reader at an airport) or used individually (as with a desktop computer fingerprint sensor).

---

identifier as an alternative to requiring the clients to produce numerous paper documents. In addition, the education programs emphasized the departments' commitments to keep biometric information from law enforcement officials. Officials found that as clients began using biometrics they realized that it made the process easier. Clients also felt better because they were not always having to prove their identity—often difficult for the poor without drivers' licenses, credit cards, and other standard forms of identification. See Appendix B, Program Reports, Social Services.

Religious Objections

In the United States, religious objections to biometrics might arise from a variety of different groups.[9] For example, certain Christians interpret biometrics to be a "Mark of the Beast." The objection is based on language in "Revelation":

> [The Beast] causeth all, both small and great, rich and poor, free and bond, to receive a mark in their right hand, or in their foreheads: And that no man might buy or sell, save that he had the mark, or the name of the beast, or the number of his name. . . . and his number is six hundred, threescore, and six. (Revelation, 13:16–18.)

Certain Christians consider the biometric to be the brand discussed in Revelation and biometric readers as the only means of viewing these brands. Similarly, M. G. "Pat" Robertson, host of "The 700 Club" and founder of The Christian Broadcasting Network, Inc., observes that the "Bible says the time is going to come when you cannot buy or sell except when a mark is placed on your hand or forehead." He expresses doubts about biometrics and notes how the technology is proceeding according to Scripture (700 Club, 1995).

Religious objections have arisen when identification programs have been implemented. In Alabama, two people objected to providing an SSN, as required under Alabama law, to apply for a driver's license. The individuals based their refusal on their sincerely held religious beliefs that prevent them from having an SSN. This case is pending in the Alabama state courts (*Alabama Lawsuit*, 2000). In the case of biometric identification, religious objections contributed, at least in part, to the failure of Alabama DMV's fingerprint program. In Alabama, groups including the Christian Coalition, Southern Christian Leadership Conference, and the American Civil Liberties Union, vigorously protested an effort to place a fingerprint biometric on all driver's licenses. In July 1997, Alabama Governor Fob James, Jr., stopped the proposed program because of these objections (Stamper, 1997). However, five other states—California, Texas, Colorado, Hawaii, and Georgia—successfully require a driver to provide a fingerprint on the driver's license, without significant public oppo-

---

[9]See Appendix B, Program Reports, Connecticut Department of Social Services and Fort Sill, Oklahoma.

sition. In West Virginia and the District of Columbia, providing a fingerprint for the license is optional. Moreover, another dozen or so states are considering or planning to use fingerprints on driver's licenses in the near future (Woodward and Smythe, 2000).

We do not expect religious objections to biometrics to be widespread, but such objections must be taken seriously because of societal and legal emphasis on respect for sincerely held religious beliefs.

BIOMETRICS RAISE SIMILAR YET DIFFERENT CONCERNS

When considering whether sociocultural concerns about biometrics are similar to or different from those raised about the use of other identifiers, we find that many of the concerns are very similar.

Informational privacy concerns are not new. The use of SSNs is a prime example of function creep—an individual's SSN is used for an array of purposes in the public and private sectors. Tracking issues are also a major concern today in part because the public has been made aware of informational commerce or the profitable use of data as a commodity.[10] For example, many retailers currently sell personal information collected from customers to data merchants, who compile and sort data from multiple sources into more comprehensive and marketable databases. At issue is not the loss of your grocery store account number but that all information associated with it, namely your food, beverage, and other purchasing habits, are now known by many unidentified people or organizations.

Religious objections are not unique to biometrics technology. Certain individuals have opposed SSNs on religious grounds.[11] In addition, the Army has had to address a variety of other religious accommodation issues, ranging from uniform attire to religious practice.

---

[10]See, e.g., *Economist* (1999). See also O'Harrow, (1999b), noting that Acxiom Corp., an Arkansas company that provides information to marketers, has amassed 135 million consumer telephone numbers, including about 20 million that are unlisted, to help identify and profile people who call toll-free lines to shop or make an inquiry.

[11]See *Bowen v. Roy*, 476 U.S. 693 (1986) (Parents contended that obtaining a SSN for their daughter would violate their Native American religious beliefs). See also *Alabama Lawsuit* (2000).

However, despite these similarities, biometric technologies raise concerns different from traditional identifiers. The concerns are a product of differences in the biometrics technology itself, the data produced by the technology, and how such data might be used. Theft of a biometric identifier poses a new set of issues.[12] If an individual's PIN for his ATM is stolen, the bank simply issues the individual another one and cancels transactions under his name made using the old PIN. However, if an individual's biometric is stolen, there must be a system in place to accept an alternative biometric or means of identification.

In addition, the data that some biometric technologies produce are, or have the potential to be, different from what is produced by traditional identifiers. Some biometric information contains medical information.[13] With technological advancements, medical information may someday be available using biometrics. Because biometrics are inherent to the individual, researchers are likely to try to link medical predispositions, behavioral types, or other characteristics to particular biometric patterns. This possibility makes biometrics different from PINs, passwords, and other generated numbers used to identify an individual.

Finally, biometrics present a greater potential for function creep because biometrics offer an ability to track individuals in a way that current passwords and PINs cannot. When biometrics replace or enhance existing security systems, their role is no different from current techniques that identify an individual or verify that a person is who he or she claims to be.[14] The difference is that unlike other

---

[12]See, e.g., Garfinkel (2000, pp. 62–65).

[13]Recent scientific research suggests that fingerprints disclose medical information. Chen (1998, pp. 221–226) states, "Certain chromosomal disorders are known to be associated with characteristic dermatoglyphic abnormalities." He specifically cites Down's syndrome, Turner's syndrome, and Klinefelter's syndrome as chromosomal disorders that cause unusual fingerprint patterns in a person. DNA is an example of a biometric that contains much more than simple identification information. However, as of 2001, DNA analysis is not sufficiently automated or quick enough to be viable for use in a biometric program.

[14]For example, several state social services agencies use biometrics to verify the identity of entitlement recipients as part of their fraud prevention programs. The problem is that some people illegally establish multiple identities and collect multiple entitlement payments, known as "double-dipping." While procuring fake documentation sufficient to establish an identity is not difficult, use of a biometric identifier

forms of identification, which are specific to particular purposes (generally a transaction of some sort), all individuals provide their biometrics as they go about their daily tasks. Faces, fingerprints, and voices are available for all to see and recognize. As a result, biometric technologies could make it feasible to capture this information and track people without their knowledge or consent. The use of biometrics as an identifier further magnifies this concern, because the biometric is not something that can be changed or discarded. For the reasons discussed above, biometrics may be perceived by some as a qualitatively different means of checking identity. Because the technology is new, however, perceptions are likely to change over time.

---

would reveal that the multiple identities all use the same biometric: a clear sign of fraud. Similarly, if a credit card were protected by a biometric, a thief could still steal it from the authorized user, but unless the thief could produce the biometrics of the authorized user for the sensor at the point of sale, the card would not be accepted.