Appendix B

PROGRAM REPORTS

The use of biometrics is increasing throughout the United States and the rest of the world. This appendix presents brief case studies of various public and private-sector entities employing biometrics to control access to facilities and computers, to prevent fraud, and to increase customer services, among other purposes.[1] The case studies pay special attention to privacy concerns and technology glitches (if any) that the Army should consider before a biometrics program can be widely implemented. This appendix concludes with case studies of other identifiers to include the DoD DNA specimen repository and the use of the SSN.

MILITARY PROGRAMS

Fort Sill Pilot Program: Biometrically Protected Smart Card

Problem: The Army sends recruits to basic training at one of five bases in the United States: Fort Sill, Oklahoma, Fort Jackson, South Carolina, Fort Leonard Wood, Missouri, Fort Knox, Kentucky, and Fort Benning, Georgia. Shortly after arrival at the base, the new recruits must buy toiletries, haircuts, and other personal items. To enable them to make these purchases, the Army issues recruits an advance on their pay. Giving these recruits several hundred dollars in cash causes concern because the money is easily lost or stolen. Thus, Fort Sill used a voucher system, while at Fort Knox, the Army

[1]For a description of some biometric applications, see, e.g., Gugliotta (1999); Hansell (1997); Rogers (various); and Mintie (various).

issued checks to the recruits and then marched them to the PX to buy money orders. These activities took hours to complete and complicated the training schedule. The Army's Training and Doctrine Command (TRADOC) and Finance Command began to look for alternative approaches. Because the Treasury Department's Financial Management Service and DoD's Defense Finance and Accounting Service (DFAS) manage government payments, they became involved in the search for solutions. The Army and Air Force Exchange Service (AAFES) also participated because it wanted to test speeding of throughputs and reduce cash handling at basic training points of sale.

Given the objective of a quick, safe, and efficient system of paying recruits, the Army decided to test three different systems of stored value cards containing digital cash:

- Smart cards that were PIN protected.
- Smart cards that were biometrically protected.
- Smart cards that were open purses, like cash.

The Army tested the biometrically protected smart cart at Fort Sill, Oklahoma (Moore, 1998). The biometric used was a fingerprint. Mellon Bank did the system integration. Identicator Technologies provided the biometric technology, with additional integration to the electronic purse done by Product Technologies, Inc.

Program: The biometric smart card pilot program began at Fort Sill in March 1998 and ran for 15 months. Determining the population to be included in the Fort Sill pilot was very straightforward, it would include all recruits arriving for basic training. Because Army basic training is a highly controlled environment, recruits have a very limited number of places at which they are allowed to spend money. The Army placed a smart card reader and fingerprint sensor at each location (points of sale) where recruits were allowed to spend money. The Army also gave a keychain-sized card reader to each drill sergeant to allow him to monitor how much money a recruit had on his card.

The first thing done with recruits arriving at Fort Sill was to verify their identity and SSNs and issue them the smart card with an

advance on their pay. Army personnel enrolled each recruit into the system using a laptop computer and sensor to scan the recruit's right index finger to obtain a digital representation of the print. The clerk also scanned the recruit's left index finger as a backup. The clerk then added cash value to the card based on an Army formula: $200 for men; $260 for women. Cards were set to expire in 60 days at which time all remaining cash transferred to the recruit's bank account, which had been established in the meantime. The Army did not keep a separate record of the fingerprint; only the serial number of the card was linked to the cardholder name.

The recruit was responsible for keeping track of his smart card, which contained his fingerprint template. At points of sale, the recruit entered his card into the card reader and placed his right or left index finger on the sensor. This template was compared to the template on the card. If they matched, the sale went through with the amount deducted from the card.

Performance: The program team had no reports of fraud and no complaints about failure to use the system. Only 10 people out of the 25,000 enrolled during the pilot program were not able to enroll. This failure rate is much lower than the advertised 1 percent for fingerprint technologies. However, these young recruits are prime candidates for fingerprint biometrics. Of those enrolled in the system, only about 3 percent failed to gain access to their card with a first fingerprint, but, when a second fingerprint was used, there was 100 percent access. The only performance issue for the system was that after several months the sensors for enrollment would wear out and "go bad." The clerks managing the system learned to recognize the signs in advance and replace the sensors as necessary.

Protections: Drill sergeants are very protective of their recruits. During informational sessions with the project team, one drill sergeant expressed concerns that recruits with fundamentalist religious beliefs might object to using the biometric on religious grounds. They were also concerned that fingerprints would be kept after recruits left and were relieved to find out that no fingerprints from this activity would be retained by the Army. Even though sales were linked by serial number to a bank, and account information and names could be drawn from this, no information was gathered about recruit purchases. The drill sergeants were also assured that the

template on the card could not be reverse-engineered into a fingerprint image. Because this pilot program did not involve personal information contained in a system of records, it had no Privacy Act implications. At the time of enrollment, each recruit received a brochure explaining the fingerprint technology.

No formal feedback was obtained from the recruits, but reportedly the drill sergeants found the program a great improvement over previous practices. The drill sergeants preferred the smart cards because of reduced risk of theft, which can be a time-consuming problem for them because they must assist with investigations, file reports, and help the recruit who has lost his money. However, the Army decided that while digital cash was a good solution, biometrics would not be used to protect the card. Experiments with open purse smart cards worked as well as those protected by a PIN or biometric but at less cost.

Lessons Learned: The program, directed from the top, was universally accepted without much difficulty. Several reasons explain this success. First, the program provided more time for training by reducing the time spent on administrative tasks. The program reduced from hours to minutes the process of paying recruits and conducting subsequent transactions for sundries, haircuts, etc. In addition, a well-thought-out educational campaign was targeted at the drill sergeants, the Army personnel who have the recruits' interests most at heart and the recruits' lives most in sight. Program managers showed some 300 drill sergeants how the technology worked, explained the limits to the information provided, and answered the sergeants' questions. Finally, the Army conducted the biometrically protected smart card program for a clearly defined purpose in a highly controlled environment with an ideal population.

All DoD training bases are now using open purse smart cards, except for the Marines at Parris Island, South Carolina, who use PINs to secure their cards.

Defense Manpower Data Center (DMDC)

The DMDC operates what is arguably DoD's largest biometric database. By way of background, the Federal Managers' Financial Integrity Act of 1982 requires federal managers to establish internal

controls to provide reasonable assurance that funds, property, and other assets are protected against fraud or other unlawful use. As a result of this legislation, DoD launched Operation Mongoose, a fraud prevention and detection initiative. Operation Mongoose exposed a number of fraud schemes and indicated that DoD needed to improve servicemember identification and verification procedures. Responding to the need for better fraud prevention measures, the acting Under Secretary of Defense (Personnel and Readiness) gave authority to the DMDC to initiate an electronic fingerprint capture policy in 1997.

In an initial pilot program, DMDC saved an estimated $8 million with 25,000 military retirees living in overseas locations. The program confirmed DMDC's suspicion that military benefits were still being collected on deceased retirees when many failed to appear to enroll their fingerprint in the new identification system (Dunn, 1998). Since 1998, the DMDC has been capturing the right index fingerprint of all active-duty, reserve, and retired military personnel as well as survivors receiving a military annuity. This potential enrollment pool is some 3 million people. The fingerprint is captured during the routine issuance (or reissuance) of military identification cards at some 900 DMDC sites. DMDC stores electronic copies of these fingerprints in a comprehensive database known as the Defense Enrollment Eligibility Reporting System (DEERS). DMDC does not store any copies of fingerprints on the actual military identification card. DEERS can be accessed if a person's identity needs to be authenticated.

U.S. Naval Criminal Investigative Service (NCIS)

NCIS has been testing a fingerprint-based system to provide secure data and voice communications with undercover agents who are unable to risk physical meetings. The small pilot began in November 1999 and concluded in February 2000. Participation in the program has been voluntary. As such, no privacy or consent issues arose with the five enrollees. Further, as NCIS agents, all have security clearances, all current and potential enrollees already have a great deal of personal information, including fingerprints, on record and are thus less likely to oppose participating in such a system.

The NCIS system consists of a number of laptops, each with an externally adapted scanner. Fingerprint data are stored in the laptop itself for verification. That is, the system does not include a central server that keeps a database of fingerprint data. The laptops' basic input/output system (BIOS) has been modified, so the computers will not operate without verification by the agent to whom the laptop has been assigned or by the system administrator.

According to one technician, during the trial these systems had only one technical problem, which involved the laptop, not the biometric element. He noted, however, that the scanners are sensitive to weather and lighting. Specifically, it is difficult to get a fingerprint reading in direct sunlight.

AN NCIS special agent involved with the test expressed his satisfaction with the system and his hope that its use would continue and expand beyond the trial period. He noted that the system has "proven itself to be reliable and do what we wanted it to do, which is to protect the information and the communications."

Face Recognition for Countersurveillance

DoD is currently working with a commercial vendor on a special project known as "Face Recognition for Countersurveillance and One-to-Many Identification of Antigovernment Factions." This project, many aspects of which are classified, has been fielded at select military installations overseas. The face recognition system is not a facial verification system but rather strives to identify the individual by performing a "one-to-many" search. In operational terms, the face recognition system takes the facial input of a subject, generates a template, compares this template to a database and then provides a list of potential candidates as an output.

Established in the mid-1990s, the vendor gained its first contract through the National Institute of Justice. Its first project assisted law enforcement officials in tracking gang members. The military saw the potential for this technology to support intelligence collection by helping to track terrorists and insurgents overseas. In 1995, the Air Force became the first military service to work with the vendor on a face recognition system. Since then, DoD has worked with the vendor on several face recognition projects.

COMMERCIAL BIOMETRIC PROGRAMS

Riverside Health System Employees Credit Union, Newport News, Virginia

The Riverside Health System includes three hospitals, 10 nursing homes, five wellness and fitness centers, three retirement communities, and 210 doctors' offices. The credit union serving this system is small, employing three staff members. In 1997, the credit union felt that the government was moving away from "dead-tree technology" and toward all-electronic transactions. As part of the process, the credit union decided to add an electronic kiosk known as the "Money Buddy"—in effect, a 24-hour automated branch. The Money Buddy allows customers to print statements of their accounts, transfer funds between accounts, apply for loans, make loan payments, and print checks for withdrawals. Money Buddy requires account numbers and fingerprints for customer access. No card is necessary. The system was in place by July 1998. Money Buddy acts as "force multiplier" for the credit union

Credit union customers include many military families: Langley AFB, Norfolk Naval Station, U.S. Coast Guard Reserve Training Center (Yorktown), the Army's Fort Eustis, and NASA's Langley Research Center are all in the Riverside Health System area. Perhaps because of the clientele's familiarity and comfort with on-base security measures, most have come to see the fingerprint system as more protective than invasive. Privacy issues have been insignificant, and both customers and management are very comfortable with the system. Account holders' fingerprint data are deleted when they close their accounts.

The system has encountered very few problems. Of 536 customers currently scanned in, about 10 are unable to use the system and use PINs instead (no card is required). Two of the 10 are a plumber and a carpenter (both military veterans) who have worn their fingers almost completely smooth. The other eight have fingerprints with horizontal lines, which apparently cause problems at the resolution level used by the fingerprint scanner. Smaller problems include climatic and occupational factors that alter individuals' fingerprints. Specifically, skin dryness that accompanies health care workers' frequent hand washings can lead to fingerprint distortions. These dry-

ness problems can be resolved by adding a bit of oil to the finger by rubbing it behind the ear.

General Services Administration (GSA) and Citibank

Since May 1999, the U.S. General Services Administration (GSA) has been using fingerprint verifications for computer workstation security as part of a nine-month pilot study. The system being tested requires no passwords or PINs and currently has 500 enrollees. Few problems have cropped up with the system, and those that have appeared are consistent with the problems found elsewhere—cuts, rings, etc., that can distort fingerprint images, whether at the time of the initial reference scan or during subsequent scans.

Some GSA employees, through their union, initially raised some concerns about privacy, but these subsided following an explanation of the system, its benefits, and the safeguards in place for employee data. Specifically, the fingerprint templates collected are encrypted when stored in the GSA database and on the associated chip card.

Visa, San Francisco, California

Visa has been exploring the use of biometrics for the past 15 years, starting with dynamic signature recognition. To date, Visa has run trials and pilot programs with most forms of biometrics, including finger, voice, hand, iris, face, and signature, in its search for what it considers the best biometrics approach to be used with their services.

Visa's operations in San Francisco use a hand geometry recognition system for their internal physical access. A program official interviewed reported there have been no failures with the hand geometry component as part of the physical security system at the Visa headquarters building. Hand geometry readers limit access to certain restricted locations within the facility.

Visa has delayed its push to use biometrics with its credit card operations for several reasons. First, Visa has been waiting for the price of biometrics systems to fall before the company pursues them in earnest. Second, Visa has yet to find the right vendor and biometrics approach. Although Visa believes a finger scan to be the proper

approach, they have not been as impressed with some of the results from trials with several vendors. Third, Visa realizes that a standard approach is necessary among credit card services, so that each does not use different vendors and different readers, which would make it difficult for business customers to implement the system.

Visa also sees a need to continue educating the public about biometrics. In its trials and market research, Visa found very little stigma associated with the use of biometrics. Visa still needs to educate the public about data protection. Another aspect of education is to inform the public, including potential criminal elements, that using a dismembered hand or finger for unauthorized access will fail.

Kroger Supermarkets, Texas

Kroger, a national supermarket chain, has recently completed a yearlong trial of fingerprint biometrics recognition in conjunction with check cashing in six of its stores. Because of the trial program's success, Kroger fielded the system in 250 stores nationwide by the first quarter of 2000.

Kroger uses a fingerprint scanning system. In each store, approximately 45 percent of all Kroger customers write checks to pay for their purchases. These customers are given the opportunity to participate in the fingerprint-scanning program. A Kroger executive said that about 8,000–10,000 customers per store participated in the test phase of the program. Kroger believes it will have similar numbers as it expands the biometric program to all of its stores. Kroger reportedly has been pleased with the program's performance as well as the overall reduction of check fraud in its stores. In the six trial stores, approximately 1,000 incidents of check fraud took place each month before Kroger implemented the system. The pilot stores have had zero incidents of check fraud since implementation. This dramatic drop in the incidence of fraud has created a large enough savings that the system should pay for itself within a year.

A Kroger executive explained that Kroger experienced very little negative reaction from customers to the use of fingerprint scanning. Customers have been pleased at the hassle-free process of paying by check. No longer do they need to show an ID card but simply put their finger on the scanner and within a second the process is over.

After a customer places his finger on the scanner, the data collected are matched to a local database on the store workstation containing the records of that store's customers. If the fingerprint is not in the store's local database, the computer searches the main Kroger database off site. If the customer is found in the main database, the individual is identified and the local database then receives the customer's record for future transactions.

Kroger was initially concerned that their senior citizen customer base might express concerns over the program but found that this group was the most enthusiastic about the biometrics system. The seniors are highly motivated with regard to fraud and security and welcomed the fingerprint scanners. Kroger did discover that seniors tend to have drier hands than younger people, and that at first hampered getting a good read on the scanner. Kroger made adjustments and now the system operates well for this customer group.

PHYSICAL ACCESS

Columbia Presbyterian Hospital, New York, N.Y.

The hospital has used a TimeLink hand geometry scanner since 1997 to monitor time and attendance and control physical access. Time and attendance measurement is the primary use of the system, which was made necessary by perceived inaccuracies in bookkeeping. In the first year of the system's operation, fraud reduction led to an estimated savings of more than $1 million. The payroll department and TimeLink maintain the system, which currently has 8,000 enrollees.

A few minor problems have been associated with the hand geometry system. Employees expressed some initial privacy concerns (e.g., "Is this taking my fingerprints?"), but the use of the system has become routine at this point, and these concerns appear to have subsided. Scanning problems can occur when the lens or scanning surface become dirty. The hospital's housekeeping department is responsible for keeping the scanning units clean. The wearing of bandages, long sleeves, and other add-ons can also distort the hand image, whether during the initial scan or during subsequent access scans. Employees' data are deleted from the system immediately with their separation from the hospital.

Universal Air Cargo Security Access System, Chicago, Illinois

The Universal Air Cargo Security Access System is a pilot program at O'Hare International Airport, the world's busiest airport. The security system is sponsored by the Federal Aviation Administration (FAA), the Chicago Department of Aviation, the American Trucking Association, and 25 trucking companies and 22 airlines. SecurCom is the systems integrator. The system features fingerprint scanners by Identix, smart cards by Schlumberger, and database software by Oracle.

Knowing that approximately 60 percent of all air cargo going through O'Hare is transported on passenger flights, airport officials and concerned parties realized this represented a potentially large security loophole through which terrorists could plant explosives or other contraband. With Universal system, truck drivers who already have a security clearance are given a biometrically encoded smart card, which contains data regarding the contents of their trucks and the number of the back door's seal. A cleared inspector encodes the card by biometrically signing off on the cargo. On arrival at the airport, both the driver and the seal are verified and biometrically accepted by the cargo attendant. The truck's payload is accepted into the airport for further processing following this verification.

The first phase of Universal's pilot, in which 12 airlines and 52 trucking companies with about 500 drivers participated, was completed in March 1999. The second phase, which will bring Newark International Airport on line as well, began in February 2000.

Other projects at O'Hare include the installation of fingerprint/smart card readers for access to the U.S. Customs area in the international terminal. SecurCom is replacing access readers at O'Hare with similar readers. Midway Airport is next in line. Currently, O'Hare's 50,000 badged employees are using a magnetic card/PIN system.

University of Georgia, Athens, Georgia

The University of Georgia has one of the longest-running biometric applications in the United States. The university started using biometrics as an identifier in 1972. Since then, it has continued to employ various biometric strategies for identification purposes.

They now use hand recognition systems for physical access purposes.

The University of Georgia saw a need to restrict access to its student dining facilities. Prior to 1972, the university used a punch card system that was ineffective and easily circumvented. In 1972, they implemented a biometric hand reader. Although problems persisted with students being able to fake the process by moving their hands while the system measured their fingers, it was an improvement over the punch cards. In 1995, they implemented a three-dimensional biometric hand geometry system. At that time, 5,400 students—those on the university's meal program—were added to the new system. Because of the success of the program, both in terms of student reaction and of curtailing unauthorized access to the dining facilities, the university decided to expand the system to address other physical access needs. The same hand geometry system is used to grant access to the 17 residence halls for 5,600 students (most of these students are in the meal program). Since 1998, the University of Georgia has required all 31,000 students to enroll in the hand geometry program, which prevents unauthorized access to the university's sport and recreation facilities.

The implementers of the system at the university were surprised at the relatively few complaints from the students. The university leaders introduced the system to the students as something "state of the art" and that they as a school were "pushing the future." They found that students were pleased to be taking part in something unique.

A university official mentioned that they do have problems with some aspects of the hand biometric system. If individuals have extremely small hands or have had broken hands, it can render the system unusable. The official also explained that for a successful reading to take place, the individual must be comfortable with the system. At the University of Georgia, many students use the system multiple times every day, so they become quickly accustomed to the procedure and have few problems.

Good Shepherd Hospital, Barrington, Illinois

In 1995, for approximately six months, the hospital used a voice recognition system to control access to the operating rooms. The

system provided so many false negatives (and irate surgeons) that it was disconnected and the magnetic card system it replaced was reinstalled. It had been thought that voice recognition would be an easy way to control access to the operating rooms without forcing surgeons to carry a card or key.

SOCIAL SERVICES

At least eight states use large-scale biometric applications in social service programs: Arizona, California, Connecticut, Illinois, Massachusetts, New Jersey, New York, and Texas.[2] We reviewed programs in Connecticut, Texas, and California. These states were chosen because of the availability of information. They are in no way a representative sampling of the states' activities. States beginning implementation of a biometric identification program include Florida, North Carolina, and Pennsylvania, while 18 more states are pursuing legislation regarding such matters.

Los Angeles Country AFIRM Program

The Los Angeles County Department of Public Social Services (DPSS) program targeted participants in the Aid to Families with Dependent Children (AFDC) and Food Stamp programs. The biometrics program is known as Automated Fingerprint Image Reporting and Match (AFIRM). It was designed to prevent fraud through duplicate participation or "double-dipping," defined as the same person enrolled in a system multiple times using multiple aliases. AFIRM uses fingerprint matching provided by PrinTrak, and EDS handles system management.

DPSS used ink-and-paper fingerprints as early as 1986. In 1988, a steering committee approved automated fingerprint matching. By 1991, DPSS launched a pilot program using automated fingerprinting. By the end of 1994, the program had been launched at all 25 DPSS district offices. The program includes 300,000 people who must be fingerprinted. These include adults receiving AFDC pay-

[2]For more information on biometrics programs operated by state social services departments, an excellent starting point is Connecticut State DSS (2000).

ments, minor parents receiving payments, and adults collecting payments for children. The biometric consists of templates of two index fingers. The data are not shared with law enforcement officials under any circumstances.

Prior to launching the program, DPSS staff explained the process to their clients and educated them as to what the system would entail. DPSS made appointments for enrollment. Those unable to make their appointments were given an additional 10 days. After that, if an adult failed to report for his appointment, adult benefits were cut off, although children's benefits continued. If an adult continued to refuse to enroll, the case was referred to the fraud units.

According to a DPSS review, most participants did not feel inconvenienced by the biometric. Rather they believed the biometric would be effective in reducing fraud, which most felt was a positive step. Of 137 cases sampled for noncompliance, 76 percent were deemed fraudulent. The DPSS felt that the biometric program saved a substantial amount of money, about $66 million in savings over 26 months.

Texas Department of Human Services (DHS)

In 1995, the Texas state legislature mandated implementation of electronic imaging as part of Texas's initiative to reduce fraud in public assistance programs. Based on TDHS's research of available electronic imaging systems, fingerprint imaging was determined to be the most reliable and affordable technology for identification verification purposes.

Texas's finger imaging program, the Lone Star Image System, was developed to deter duplicate participation in the Food Stamp and Temporary Assistance for Needy Families (TANF) programs. A pilot project of the Lone Star Image System began in October 1996 in 10 offices in the San Antonio region, enrolling more than 85,000 clients.

Based on the success of the San Antonio pilot program, federal approval for full statewide implementation was given in May 1998 and implementation was completed in August 1999.

Adults (over 18 years of age) and minor heads of household receiving Food Stamps or TANF are required to provide finger images when

they apply or recertify. Fingerprint imaging of two index fingers and a digital photograph of the individual constitute the enrollment record. More than 400 Lone Star Image System enrollment stations can be found throughout the state, including some mobile stations at temporary offices. Finger image enrollments are routinely purged after six months of inactivity.

Although the system has not caught many individuals committing fraud, TDHS estimates that the system saves $6.36 million each year by deterring potential duplicate recipients. TDHS estimates that the incidence of duplicate participation in the Food Stamp program is about one half of one percent of the total caseload.

In 1997, the Texas legislature instructed TDHS to plan a pilot project allowing clients to provide finger images instead of a PIN at the point of sale when accessing benefits under the Lone Star Card/electronic benefit transfer (EBT) program. This program employs a debit card instead of Food Stamp coupons or paper checks in distributing Food Stamp and TANF benefits. However, in 1999, the Texas legislature did not approve funding for the pilot project, stating that the technology of biometrics at point of sale was not sufficiently mainstream at the time.

Results of a survey conducted by TDHS showed that 89 percent of program participants thought biometrics were a good idea and 81 percent think using finger images instead of PINs at point of sale is a good idea.

Lack of standardization among the biometric venders is a major problem. For example, DHS has worked with Kroger supermarkets to develop a finger imaging at point-of-sale joint pilot project. However, interoperability problems—merging TDHS's system with Kroger's existing finger imaging check authorization program would require Kroger to use a separate fingerprint scanner—added cost and complexity to the process.

Connecticut Department of Social Services (DSS)

Legislation drafted in 1995 funded the study and eventual deployment of a fingerprint biometric to prevent welfare fraud. Connecticut wanted to create a system that would deter dual enrollments,

including enrollments in neighboring states. It is not uncommon for the same person to illegally participate in several states' entitlement programs at the same time through the use of aliases and forged identification documents. Accordingly, DSS selected a biometric with an eye toward compatibility with the neighboring states of New York and New Jersey. As it turned out, the states' templates are not compatible, making interstate comparisons somewhat complicated.

Connecticut has 24,000 general-assistance enrollees and 60,000 AFDC clients in its system. The program was implemented in 16 regional offices, 20 town general-assistance offices, and the DSS Hartford office. It uses centralized image storage and retrieval. The cards can be used in one-to-one verification or one-to-many identification using the network of databases.

In addition to the fingerprints stored, each card and file carried a photograph and signature of the recipient that can be manually matched by social services staff to verify the recipient.

Prior to implementing its program, the DSS conducted an extensive education campaign. Despite these efforts, some members of the legislature vigorously opposed the program. In addition, since its establishment, the state has received three refusals to participate made on religious grounds. These cases were resolved by an administrative decision to allow the three persons to use alternative identification means. DSS conducted a survey of program participants and found that the majority approve of the Connecticut biometric program. More than 80 percent of those responding stated that they favored the program.

Connecticut's vision for biometrics includes using the ID card in EBT transactions, point-of-sale devices for disbursement of medical services, and distribution of Food Stamp benefits through food retailers.

DSS estimated its first year operating costs at $2.6 million with an estimated savings (from deterrence) of $7.5 million.

Illinois Department of Human Services

In 1994, the Illinois legislature approved a study of the use of biometric scanning to detect and deter fraud in programs administered by the Illinois Department of Public Aid. Officials tested retinal

scanning in two offices downstate and fingerprint scanning in three Chicago offices. Fingerprints were required in the test offices for cash disbursements but not for Food Stamps or medical payments. The department was very satisfied with the fingerprint system and dissatisfied with the retina scanning system.

In July 1997, the department was partially incorporated into the Illinois Department of Human Services (DHS). This organizational change led to changes in information technology personnel. Currently, the system is partially operational, and DHS is pursuing a decision to expand electronic fingerprinting statewide. A full-time staff member has been hired to provide technical support for the system.[3]

Social Services Summary

All three programs have had to deal with privacy concerns, and each had a handful of objections raised on privacy grounds. Each of the databases was explicitly declared to be inaccessible by law enforcement officials. All use secure designs to protect against hackers and have procedures in place to prevent unauthorized disclosure of information. Connecticut's DSS believes that answers to privacy concerns can be found in the careful packaging of the implementation legislation, use of the biometric only for the social services program integrity, and a secure design of the biometric system to protect from unauthorized disclosure.

Use of biometrics in the social services sector will continue to expand. States are seeking to make their systems more robust, both in terms of interstate compatibility and with additional applications.

IMMIGRATION AND LAW ENFORCEMENT

U.S. Immigration and Naturalization Service (INS)

INS deployed its Immigration and Naturalization Service Passenger Accelerated Service System (INSPASS) in 1993. INSPASS is based on hand geometry (but it was also designed to allow the use of finger-

[3]See also Illinois State DHS (1997).

prints as an alternative). The prototype installations were at JFK, Newark, and Pearson (Toronto) International Airports. Additional deployments include Miami, Los Angeles, San Francisco, Dulles, Vancouver, B.C., and other high-volume international airports.

More than 85,000 people are currently enrolled in this frequent international traveler program, and more than 200,000 transactions have been processed since its installation. INS, in cooperation with the Department of State, determines the rules for who may participate in INSPASS. Citizens of the United States, Canada, Bermuda, legal permanent residents of the United States, most landed immigrants in Canada, and Visa Waiver Pilot Program countries with visa classifications B-1, D-1, TN, WB, and some nonimmigrants in classes A, E, G, and L who travel to the United States on business three or more times a year or who are diplomats, representatives of international organizations, or airline crews from pilot program nations may voluntarily enroll in the INSPASS Program. Access to INSPASS is not available to anyone with a criminal record or to aliens who require a waiver of inadmissibility to enter the United States.

As of last year, approximately 35,000 American and foreign users have voluntarily registered in the system. Los Angeles International Airport alone enrolls 40–50 new users per day, and 40–100 users take advantage of the LAX INSPASS kiosk each day. Roughly 25,000 international passengers go through INS control at LAX daily. Gaining border access with INSPASS typically takes less than one minute, while waiting in line for manual passport stamping can take up to 45 minutes for U.S. citizens and two hours for foreigners.

Travelers who register false reads are sent to see an INS inspector and can be locked out of the system for four hours. There is a problem with people who have small hands (e.g., Japanese flight attendants have been particularly problematic at LAX). People who have no right hands use their left hands upside-down.

Sarasota County Detention Center, Sarasota, Florida

Since 1998, the Sarasota County Detention Center has used an iris recognition system, created by IriScan, to verify the identities of its approximately 750 inmates. As inmates are brought into the detention center, a device scans their irises, and they are enrolled in the

system. Currently, the detention center uses the system only to verify its inmates when they enter and when they leave.

Within the detention center, the inmates also use photo ID cards for internal verification. In the past, inmates would steal the cards of those inmates about to be released in an attempt to assume their identity and escape. Since the IriScan system was implemented, eight inmates have been caught by the iris recognition system while trying to escape using stolen identities. Another individual was falsely arrested and released when the iris scan revealed he was not the person the police wanted—the wanted suspect was a recently released inmate with his iris template still on file.

The Sarasota County Detention Center is pleased with the system. The whole system, including implementation, cost around $6,000 and has already proved its value through the foiled escapes. The system also reduces the need to have forensic experts assist in proving the identity of an individual by reading fingerprints. The iris recognition system takes less than a second to verify the individual and provides positive identification at any time of the day.

The database allows for input into a comment section where data concerning warrants can be maintained, which helped the detention center identify an individual who had three additional outstanding warrants.

DoD DNA Specimen Repository for Remains Identification

The DNA Repository for Remains Identification along with the Armed Forces DNA Identification Laboratory make up the DoD DNA Registry.[4] The DNA Registry, a Division of the Office of the Armed Forces Medical Examiner, helps the military identify remains of soldiers killed in combat or missing in action. High-velocity weapons and the lethality of the modern battlefield often destroy any chances of using fingerprints or dental records. DNA, however, can almost always be used to identify remains. Although most times the armed forces can identify the dead based on various records, DNA identifi-

[4]For an excellent discussion of the DoD DNA Registry, see Weedn (1998). Dr. Weedn was the founder and for seven years the program manager of the DoD DNA Registry.

cation provides closure for the family and the biological proof of death required by life insurance companies.

This issue came to a head as the military prepared for Operation Desert Storm with the potential for large numbers of casualties. The Dover AFB, Delaware, mortuary facilities were expanded, but medical officials were concerned about the ability to identify the dead. DNA techniques had been pursued by the military in its efforts to identify servicemembers missing in action from Vietnam, Korea, and even World War II, but this was a slow process that required the military to find close relatives and obtain samples from them in an attempt to match them to DNA samples from the deceased.

Army pathologists were convinced that the need to identify large numbers of dead service personnel had to be addressed and that a military DNA registry could provide a suitable solution. The Army leadership also became convinced of the utility of such a registry and lobbied for it. In December 1991, authorization and appropriations for the DNA program were received. Since June 1992, DoD has required all military inductees and all active-duty and reserve personnel to provide DNA samples for its DNA Repository at the time of enlistment, reenlistment, annual physical, or preparation for operational deployment. The DNA Repository also contains samples from civilians and foreign nationals who work with the U.S. military in arenas of conflict. DoD stores the samples in freezers at the DNA Specimen Repository in Gaithersburg, Maryland.

Implementation of the program in the Army, which is the executive agent of the DNA program for DoD, was not without controversy. Everyone was concerned about privacy, from DoD officials to policymakers to the media. The program office began to hold meetings to educate military personnel about the purpose of the program and the privacy protections that would be used to ensure that DNA data would not be otherwise employed. The education campaign worked, and at all levels military personnel have participated in the program. To date, those who have refused to participate in the DNA registry have been forced to leave the service.[5] As of 1998, only three

[5]On March 17, 1997, a DoD directive permitted the armed service branches to exempt certain members from the mandatory DNA collection requirement to accommodate religious practices.

servicemembers have refused to submit samples, as opposed to some 1.3 million servicemembers who have complied.[6]

Undoubtedly, a number of servicemembers are unwilling participants but have chosen to trust the Army rather than leave the service. In addition to the education campaign, other announcements had to be made about the program. In particular, on June 14, 1995, DoD placed "system of records" notice in the *Federal Register* announcing the establishment of this new system containing personal information (Weedn, 1998, p. 354). This announcement, required by the Privacy Act, needed to be approved by DoD's Privacy Board. It was, after deliberations that took 18 months.

Another major issue for the program was how long to keep the DNA records. One might assume that they would just be pulled when a servicemember leaves the military, but apparently similarity of servicemembers' names or SSNs as well as clerical error raised the risk of pulling the wrong record. It is also time-consuming to search the repository continually for individual records, particularly when the records number more than 3 million.

Originally, DoD's policy called for destruction of DNA records after 75 years. However, in 1996, DoD changed the destruction schedule to 50 years, to be compatible with standards for military health records.[7] This 50-year period ensures that no servicemember remains in the armed forces when his DNA record is pulled from the database. Also, in 1996, DoD amended its policy to permit servicemembers to request that their DNA samples be destroyed when they leave the service. In other words, servicemembers can opt out of the database. Once a servicemember makes such a request, DoD has six months to destroy the DNA records.

DoD's strict policy on sharing of the specimens ensures that DNA specimens can only be used for

- remains identification

---

[6]See Weedn (1998, p. 354) See also *Mayfield v. Dalton*, 901 F.Supp. (D. Hawaii 1995) (dismissing all the claims of two Marines who refused to participate in DNA program on grounds that it infringed on their constitutionally protected privacy rights).

[7]Apparently, the time period was changed as a "technical correction" (Weedn, 1998, p. 351).

- internal quality-control purposes
- consensual uses, and
- other limited uses as compelled by law.

This last category includes a court order authorizing sharing investigation or the approval of the DoD General Counsel or Assistant Secretary of Defense for Health Affairs for prosecution of a felony. The specimens cannot be used without consent for any other purpose, such as paternity suits or genetic testing. In addition, the specimens are considered confidential medical information and are covered by federal laws and military regulations on privacy. This policy has been tested by numerous federal agencies who have asked for access to the data, primarily for law enforcement purposes.

SOCIAL SECURITY

The Use and Misuse of Social Security Numbers

The controversial history of Social Security numbers (SSNs) provides an important case study on the subject of citizens' privacy rights vis-à-vis federal, state, and local government. When first devised in 1935, the SSN was issued to workers exclusively for Social Security Administration (SSA) accounting purposes. The cards as originally issued noted, "Not for Identification Purposes." By 1943, however, an Executive Order required that "all Federal components use the SSN 'exclusively' whenever the component found it advisable to set up a new identification system for individuals." (U.S. Social Security Administration, 1998.)[8] Since then, the SSN has been at the center of a public debate about whether there should be a U.S. national identification card.

In 1999, the U.S. General Accounting Office (GAO) submitted a report detailing government and commercial use of SSNs to a House subcommittee. At that time, Congress was considering legislation regulating the use of SSNs in response to public concerns about organizational use of SSNs and the role of the SSN in the growing phenomenon of identity theft (GAO, 1999, p. 1). The GAO report

[8]Information on the history of the SSN is available at http://www.ssa.gov/history.

found that "no single federal law regulates the overall use of SSNs." Rather, a number of laws require the use of SSNs for specific applications (e.g., Medicaid, Food Stamps, commercial driver's licensing programs), while other laws restrict the SSNs' use. Significantly, the GAO found that "no federal law . . . imposes broad restrictions on businesses' and state and local governments' use of SSNs when that use is unrelated to a specific federal requirement." (GAO, 1999, p. 2.)[9]

The use of the SSN has attracted increasing legislative attention as high-speed data processing systems have made SSN use more commonplace in both the public and private sectors. Organizations and agencies that GAO consulted cited the usefulness of the SSN as an identifier that transcends state boundaries and name changes and is easily used for transferring data among bodies (*e.g.*, credit bureaus to banks, HMOs to hospitals). These organizations and agencies made their belief clear to the GAO that "their entities would be negatively affected if federal laws were enacted restricting use of SSNs" (GAO, 1999, p. 12).

It is this very ease of data transfer, however, that has led some members of Congress and various watchdog groups to support legislation restricting the use of SSNs and making identity theft a crime.[10] Depending on which side one believes, the information revolution heralds either a new era of convenience, ease of transaction, and security or the advent of a governmental-industrial Big Brother with far more knowledge about U.S. citizens than is warranted.

---

[9] For examples of people and institutions opposed to the widespread use of SSNs or other forms of national identification, see Moore (1997) and SCAN (2000). See Miller and Moore (1995) and Garfinkel (2000, pp. 16–35) for a discussion of the SSN and function creep.

[10] See, e.g., Identity Theft and Assumption Deterrence Act of 1998 (P.L. 105-318).