Establishing Identity

A focus on technology

by Tod Newcombe

The prison population of Middlesex County, Mass., has grown significantly in recent years, but the size of its correctional staff has not kept pace. The disparity has led to problems tracking prisoners' identities, including mixups where wrong prisoners were transported to court for arraignments and trials. "That screws up court dates, transportation, and wastes time," remarked Alex Leone, information technology director for the Middlesex County Sheriff's Department.

To ensure the accuracy of identification procedures for prisoners and detainees, the county has installed a $1.3 million fingerprint identification and tracking system that will use a database of text information, fingerprint images and mug shot photos to help personnel accurately identify prisoners. Leone said the technology is well worth the investment — primarily for safety and efficiency reasons. "The bottom line," he said, "is that we want to make sure we are not releasing the wrong person back into society."

Tod Newcombe is Associate Editor of Government Technology. *This article appeared in their March 1997 issue. Copyright © 1997 by* Government Technology, *it is reprinted with permission.*

Since the 1980s, law enforcement agencies have been using computers to match fingerprints taken from crime scenes with prints from established criminal files. The early systems ran on mainframes and were too expensive for all but the largest law enforcement agencies in the country. With lower hardware and software costs, however, owning an automated fingerprint identification system has become less of an issue for mid-sized agencies.

At the same time, new forms of biometric technology have appeared, as have new uses for identification technology. Beside prisons and police, a number of federal and state government agencies are beginning to use identification technology to help recognize and track individuals.

The Immigration and Naturalization Service is developing a database of fingerprints for all illegal aliens intercepted entering the United States from Mexico. The agency also runs fingerprint checks on individuals who apply for citizenship. In addition, counties and states are investing heavily in identification technology to cut down on welfare fraud.

All these identification programs benefit from rapid improvements in software that can match biometric identifiers, such as fingerprints, hands and retinas; computers that can process huge database searches in seconds; and networks that enable dozens, even hundreds, of locations to transmit search requests without long waits for results.

Privacy

But as the pool of individuals required to use these systems grows, so do worries about privacy. Meanwhile, concerns have been raised about the proliferation of computerized identification systems and what some people consider the inevitable linking of databases.

In his article, "Touching Big Brother," a British professor, Simon G. Davies, warns that "from the perspective of individuals, any move toward a biometric identifier carries enormous risk." He goes on to say that "if a scheme is applied across multiple organizations, behavior in relation to one organization might lead to a domino effect of 'cross enforcement' activities, involving suspension of entitlements or benefits by other organizations. Individuals who cannot, or will not, use the prescribed system may become outcasts on the edge of society."

Identifying the Right Technology

Using biometrics to identify a person is nothing new. It has been going on ever since the ancient Egyptians started keeping measurements of their pharaohs. In the 20th century we have learned how to scan and measure a range of unique identifiers of the body, from microscopic blood vessels that appear on the retina of the eye and the geometry of the hand, to ridges on the surface of the skin, or the aural patterns of the voice.

Computers have raised the sophistication and accuracy of biometric identification to new levels. According to Davies, computers that scan a retina are extremely accurate. Studies show fingerprint identification systems can be accurate 99.9 percent of the time. Performance has also improved significantly in recent years. Workstation computers can find and match fingerprint images in a few seconds, making identification a realtime operation.

Federal, state and local governments have tested just about every type of biometric technology that is commercially available. According to a report released by the General Accounting Office (GAO) on identification technology, the Federal Bureau of Prisons uses hand geometry to identify staff, inmates, and even visitors. Hand geometry systems measure the height of the hand, the distance between knuckles and other information that is converted into an algorithm. At one prison site, the geometry system has checked over 200,000 hands without an error.

Prisons have also adopted retina scans, primarily to identify inmates when they are released from custody. Retinal-scan devices capture the unique pattern of blood vessels in the person's eye. The scanned image is turned into an algorithm that can be stored by the computer. Identification usually works when an individual enters a personal identification number (PIN) into the computer and then places his or her eye over a lens, which aligns the eye for proper scanning. If the blood-vessel algorithm and PIN match, the person is identified. According to GAO, an eye pattern is affected only by a serious eye illness or injury, such as a detached retina.

> ***"Computers have raised the sophistication and accuracy of biometric identification to new levels."***

Voice verification relies on identifying a person according to certain vocal characteristics, such as bass and treble tones, vibration in the larynx, throat and nasal tones and air pressure. These characteristics give individuals a unique sound that the computer can convert into an algorithm for identification. While less common than other forms of biometric identification, at least one local government is known to use it to control employee access and prevent thefts at one of its maintenance buildings.

Fingerprinting has become the dominant form of biometric identification today. It's considered the most feasible to operate on a large-scale basis, which is why electronic fingerprinting is growing among non-criminal applications. With no two fingerprints alike, agencies can easily capture a set of prints using small scanners that digitize fingerprints by automatically creating a spatial map of the unique arches, loops and whorl patterns on each print. The computer matches prints by scoring how close a potential match comes to the print, based on the information stored in the database.

A Standard Is Chosen

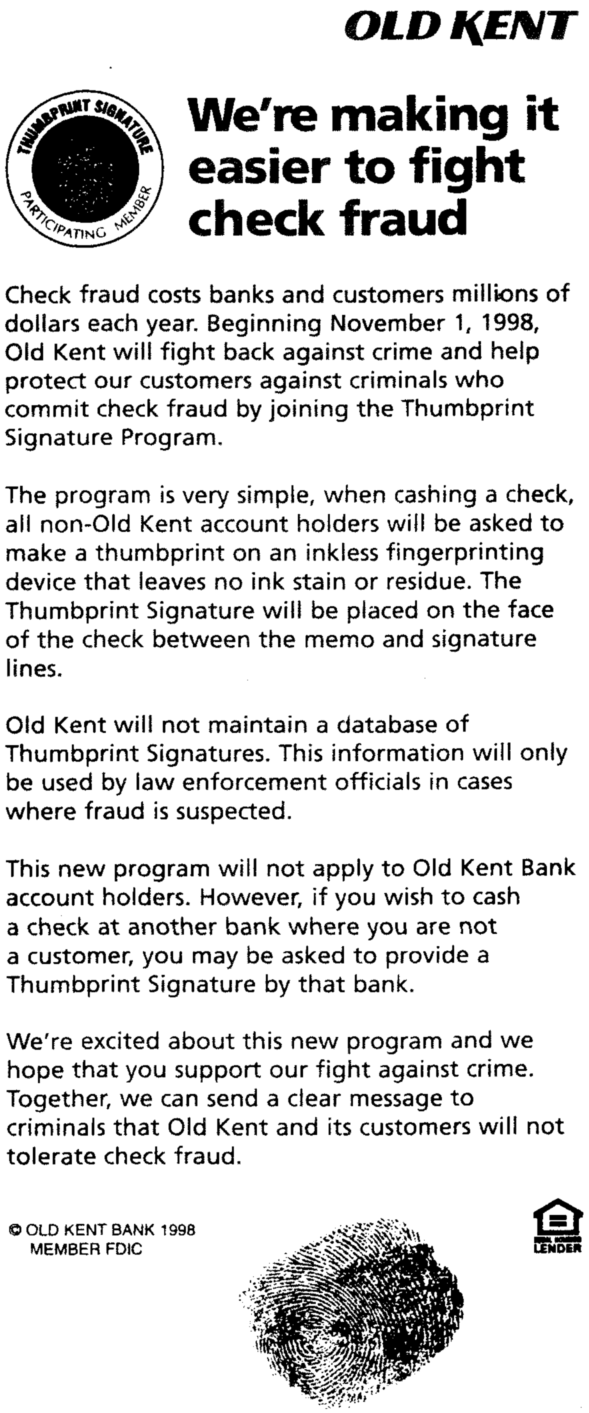
The Middlesex County Sheriff's Department went with a fingerprint identification system because the technology has been proven to work. "It's something reliable we felt we could stick with," said Leone. "Maybe down the road the retina scan will be the way to go, but we wanted to go with something proven among law enforcement agencies."

The county's identification system runs on Windows NT and was built and installed by Unisys Corp. using software from The MCL Group, a firm that specializes in tracking systems. The identification system operates on a wide area network that links the county's prison in Billerica with its jail in Cambridge over a T1 line. The system, known as POSITRAC, supports 110 users and includes a sophisticated inmate tracking system.

Middlesex County also chose fingerprint identification because the state and neighboring jurisdictions use or plan to install the same technology. "We want to hook up to the state police electronically," said Leone, "so we can share fingerprint images." He explained that if a detainee is also wanted by the state police the county can transfer him and avoid the high cost of incarceration.

Connecticut has selected fingerprint identification for the same reason, although its use for the technology is much different. In January 1996 the Department of Social Services (DSS) installed a fingerprint identification system to eliminate dual-enrolments in the state's welfare assistance programs.

A member of *The Social Contract* staff recently was asked to leave a thumbprint sample on a check being cashed. He was given this explanation of the program:



OLD KENT

We're making it easier to fight check fraud

Check fraud costs banks and customers millions of dollars each year. Beginning November 1, 1998, Old Kent will fight back against crime and help protect our customers against criminals who commit check fraud by joining the Thumbprint Signature Program.

The program is very simple, when cashing a check, all non-Old Kent account holders will be asked to make a thumbprint on an inkless fingerprinting device that leaves no ink stain or residue. The Thumbprint Signature will be placed on the face of the check between the memo and signature lines.

Old Kent will not maintain a database of Thumbprint Signatures. This information will only be used by law enforcement officials in cases where fraud is suspected.

This new program will not apply to Old Kent Bank account holders. However, if you wish to cash a check at another bank where you are not a customer, you may be asked to provide a Thumbprint Signature by that bank.

We're excited about this new program and we hope that you support our fight against crime. Together, we can send a clear message to criminals that Old Kent and its customers will not tolerate check fraud.

© OLD KENT BANK 1998
MEMBER FDIC

According to David Mintie, digital imaging coordinator for DSS, a prime reason the state chose fingerprinting over other biometric technologies was to share the images with other states. "Connecticut is very interested in matching our finger images with neighboring states, such as New York and New Jersey," he said.

Connecticut's decision to identify welfare recipients is part of a growing trend in state and county government. Hoping to eliminate what they believe to be a significant problem with welfare programs, states are pouring millions of dollars into identification systems. Various law enforcement officials estimate the losses from fraud in existing programs, such as food stamps, to be as high as 10 percent annually, but this number has not been verified, according to the GAO. In Los Angeles County, where fingerprint identification technology was first used with welfare recipients, an independent study has shown a fraud rate of between 1.5 percent and 2 percent.

Even with these low numbers, governments consider identification systems a worthwhile investment and fingerprinting the choice for identifying recipients. "We decided to use finger imaging largely because it was the single biometric that was emerging in the human services field," said Mintie. He pointed to its use in virtually every other state welfare agency that had an identification system installed or under development. Mintie added that not only was finger imaging a proven technology, but it worked with large databases. "A lot of other biometrics have been demonstrated in smaller situations, such as access control, but they really haven't been proven with a larger database," he said.

Since the program began, Connecticut has fingerprinted 86,000 recipients in its General Assistance and Aid to Families with Dependent Children programs.

How Much Identification Do We Need?

While states and counties are installing biometric identification systems to deter double-dippers in their welfare programs, the federal government is considering the use of identification technology as part of a national electronic benefits transfer program. This would allow welfare recipients to receive cash payments and to purchase food using an access card that is similar to a bank's cash and credit cards.

Citing several instances of fraud already uncovered in the limited number of EBT programs operating around the country, GAO has stated that an "EBT program without the enhanced security of biometric verification raises a genuine concern about the potential for increased costs and losses." GAO goes on to say that it optimistically believes "commercial and banking entities that use debit and credit cards will implement biometric safeguards, such as fingerprinting, to protect their customers and themselves."

Federal interest in expanding identification of citizens has been on and off the burners for some time. Beginning in the 1970s and as recently as 1990, Congress and other federal agencies have considered using biometric identification for various purposes. The Biometric Identification Act of 1990 proposed a mandatory biometric identification system that would have established a pilot program to evaluate the effectiveness of a national biometric driver's license system. The legislation was never enacted, but parts of it ended up in the Immigration Act of 1990.

> ***"While Congress has repeatedly turned down attempts to broaden the use of biometric identification, clearly its use is growing."***

While Congress has repeatedly turned down attempts to broaden the use of biometric identification, clearly its use is growing. Despite government's reassurance that identification data in a social service program won't be shared with a law enforcement database, evidence may prove otherwise. Davies pointed out that the history of identification systems throughout the world provides evidence of "function creep" where new uses of identification data are found that were not announced or even intended when the system began.

At the same time, however, public concerns about using biometric identification on a broader scale may be changing to accept greater fraud control and security. Attitudes about traditional notions of privacy are also shifting, making identification systems more acceptable. Already a number of countries are instituting national identification systems based on biometric technology. In the United States, surveys among welfare recipients show a high rate of acceptance for identification systems that prove they can curb fraud. If used prudently and according to public standards of privacy, biometric technology may become our prevalent form of identification in the 21st century. TSC

Screening People Electronically

Technical successes and political failures

by David Simcox

A Mexican citizen driving a late model car bearing a machine-readable border crossing tag approaches a U.S. border checkpoint, using the tag-only express inspection lane. A scanner "reads" the electronic tag on her car and relays an image to U.S. immigration and customs computers at the inspection point. It shows the owner's name, photo, personal data and specifics on the car, as well as any significant antecedents.

Most vehicles get an immediate wave through as intended when the computer confirms the identity of the car, the occupant, and the validity of her visa or border crossing card. This vehicle, however, is stopped. An immigration official has noticed that the computerized photo of the authorized vehicle operator does not match the driver. Further inspection confirms that the driver, who states she borrowed the car, lacks documents to enter and that she has made unauthorized use of Medicaid in past visits. She is returned to Mexico and the person lending the car is investigated for violating the conditions of the electronic tag. A look out notice is appended to that tag number in the computer's data.

The needs for secure identification in so many areas of U.S. society, and the technical advances to answer those needs, are very much the casualties of a lack of political will.

Another new INS system at ports of entry (INSPASS) uses computer matching of hand geometry to admit frequent foreign visitors to the United States, speeding the process and reducing the number of inspectors needed.

At its southern California stations, the U.S. Border Patrol now uses automated fingerprint identification systems (AFIS) to record all apprehended illegal aliens. The fingerprint files, more than a million of them captured in the first year of the IDENT system's operation, are valuable for tracking criminal aliens and multiple violators, and for intelligence on border crossing routes and methods.

Such advances as these in identification science and instant computer verification that have made checking the crush of entrants more efficient and credible also give new hope for developing more comprehensive high-tech systems foı instantly distinguishing between those who do not belong in the United States and those who do.

Rising costs of traditional methods, public concern over illegal immigration and alien crime, and diminished concern over possible invasions of privacy have energized the search for better automated systems to protect the borders. The success of Proposition 187 in California in 1994 focused Congress on illegal immigration as never before. Nevertheless, Washington's political will to use these technologies still lags behind the parade of new opportunities they are presenting. Latent ambivalence

David Simcox is chairman of the Policy Board of the Center for Immigration Studies, a Washington, D.C. think tank. He is a frequent author on immigration, population and identification subjects, including the 1989 Center for Immigration Studies publication, "Secure Identification: A National Need – A Must for Immigration Control."