



Biometrics: Tomorrow's Technology Today

The biometrics industry believes states will jump on board as costs drop

By Jenny Price

With a simple scan of a fingerprint or eyes, the government can match an individual's identity against a database of thousands to find out if he is who he says he is.

The technology isn't limited to the imaginary realm of TV shows and spy movies; it already exists in the real world. Companies are manufacturing and selling biometric devices that can identify people through scans of fingerprints, hands, irises, retinas and faces or by analyzing a voice or signature.

Some corporations in the United States rely on fingerprint scanners or similar technology for employees to access certain offices or to log onto computers. In Japan, major banks use biometric identification on automated teller machines—by scanning either fingers or the palm of a hand—to identify account holders. And a University of Wisconsin professor is in the early stages of researching electrocardiogram (ECG) recognition—capturing the heart’s unique electrical activity—as a possible alternative to the biometric technologies already in the marketplace.

There are benefits to using such technologies for figuring out who someone is or determining if they are who they claim to be. Unlike a password or PIN, a person’s biometric characteristics can’t be forgotten, lost or stolen, experts contend.

“It’s more reliable than a Social Security number or any other data that’s out there,” said Jim Jasinski, executive vice president for California-based Cogent Systems, which supplies fingerprint imaging systems to government and commercial customers.

Still, state governments have taken smaller and slower steps toward adopting biometrics because of concerns about cost, logistics and security.

Fingerprints to Stop Fraud

Some states have explored using fingerprint identification to confirm the identity of parolees or sex offenders during their required check-in visits. Arizona, California, Connecticut, New York and Texas have established statewide systems to scan the fingerprints of applicants for public assistance.

Supporters say the technology catches people who try to “double dip” by creating false identities.

Richard Nawrot, who runs New York’s 10-year-old automated fingerprint system for the state’s Office of Temporary and Disability Assistance, says there have been about 1,700 fraud cases over the last decade, but the system’s real value is in deterrence.

“We’ve saved a lot of money by preventing the fraud to begin with,” he said.

But opponents argue such systems are not cost-effective and could even discourage those in need from coming forward for help because of the stigma attached to giving a fingerprint.

In Texas, where the state has used fingerprint scanning on food stamp applicants since 1999, former state Rep. Glen Maxey unsuccessfully attempted to end the program during his 10-year tenure in the House of Representatives.

“The studies were showing that we were spending several millions of dollars a year on doing it and find-

ing only a pittance of actual fraud,” he said. “The term I used over and over during the debate [was]: ‘Is the juice worth the squeeze?’”

California Assemblywoman Sally Lieber echoed Maxey’s arguments in criticizing her state’s \$11 million a year fingerprint imaging system for public assistance applicants that began in 2000.

“I think any state that has not wasted money on one of these systems yet should stop themselves before they do,” she said. “I’m sure it’s considered a positive thing by the corporations that make this technology, but it’s not really our need to keep them afloat.”

But Andrew Roth, a spokesman for the California Department of Social Services says spending \$8 million to operate the system is a good investment when compared with the \$387 million a month the agency distributes in benefits.

“We view that as a kind of insurance,” Roth said.

The Texas Health and Human Services Commission also is convinced the system is worth the \$2.5 million a year it costs to operate, and spokeswoman Jennifer Harris says the agency estimates the state saves between \$6

million and \$11 million a year by deterring fraud, numbers critics dispute. Texas is also looking into using biometric technology to detect fraudulent Medicaid billing and possibly embedding personal data onto a universal benefits card—sometimes called a “smart card”—for multiple public assistance programs.

Cost Plays Role in Becoming Biometric

Money has kept some states from wading into biometrics altogether. Illinois, Maryland, Michigan and North Carolina all rejected statewide use of the technology after determining it was not cost-effective.

But players in the biometric industry contend states will jump on board as costs continue to drop.

“It’s got to be cost-effective,” said Bud Yanak, vice president of marketing for New Jersey-based BIO-key International, which supplies biometric finger identification technology to private industry and government. “Eight years ago, biometrics weren’t as cheap and available as they are today.”

Yanak noted that several computer companies now ship laptops equipped with fingerprint readers, something that wasn’t available a few years ago.

Iridian Technologies, also based in New Jersey, has been making iris recognition technology for about 10 years. A few years ago, the cameras for photographing the eyes cost upwards of \$20,000, said Frank Fitzsimons, the company’s president and CEO.

Now, a desktop camera for iris recognition can cost as little as \$200, he said.

“It’s more reliable than a Social Security number or any other data that’s out there.”

—Jim Jasinski, executive vice president for California-based Cogent Systems

For the last year and a half, Connecticut has used iris recognition to verify which inspectors are conducting emission testing at private garages after having a problem with fraud, Fitzsimmons said.

State motor vehicle departments are also showing some interest in biometrics to eliminate issuance of false and multiple identifications, he said. Iridian recently received a request for information from the Illinois Department of Motor Vehicles.

Security, New Technologies on the Horizon

The use of biometric technologies has been fueled, in large part, by the push for new security measures in the wake of the Sept. 11 terrorist attacks, particularly for travel documents used for border entry and exit, said David Mintie, editor for the online newsletter “Biometric Watch.”

Players in the biometric industry contend states will jump on board as costs continue to drop.

The federal government is working on plans to develop biometric passports, which would include digital photographs and fingerprints, and Mintie predicts biometrics will become a multi-billion dollar industry.

But Mintie, who directed the Biometric Identification Project for the Connecticut Department of Social Services from 1995 to 2003, said the question of how the information collected will be protected is looming over the push for new technologies.

There are legitimate, ongoing concerns about having biometric data stored in any kind of database and whether individual privacy can be compromised, he said.

“How carefully is that data going to be safeguarded? This is going to be a big, big issue,” Mintie said. “It doesn’t matter whether you’re in government or the private sector.”

—Jenny Price is a former Associated Press statehouse reporter. She is now a freelance writer based in Madison, Wis.

Biometric Resources

Biometric Watch—online newsletter and resource about new products, new applications, case studies and successes and challenges in the biometrics industry, as well as a glossary of biometric terms.

www.biometricwatch.com/Glossary/glossary.htm

The Biometric Foundation—industry group providing research and education.

www.biometricfoundation.org

The Center for Identification Technology Research of West Virginia University—center chartered by the National Science Foundation; in 1998, WVU became first university to offer undergraduate degree in forensic and biometric identification.

www.citer.wvu.edu

The International Biometric Industry Association—trade group whose members account for over 80 percent of biometric manufacturing revenues worldwide.

www.ibia.org

