



## Your Face or Mine? Ask a Computer

By: William M. Bulkeley

### Feature-Recognition Systems Match Facial 'Landmarks' To Determine Positive ID.

Computerized face recognition, a staple of spy movies and science fiction, is increasingly part of the real world.

In Houston and Dallas, people who can't afford to maintain bank accounts are able to cash checks at kiosks that scan their faces and dispense money. In London, the Newham neighborhood attributes a 40% drop in crime to equipping its surveillance-camera network with face-recognition software trained to identify neighborhood criminals. In Israel, police are installing a system that uses a combination of computerized face recognition, hand-geometry scanning and "smart" cards in an effort to speed the passage of Palestinian day laborers from Gaza into Israel.

Five years ago, face recognition looked too complex and expensive to have real-world applications, given the meager visual capabilities of computers. Since then, researchers have made huge strides by limiting the amount of data needed to define a face. Even personal computers are now fast enough to scan millions of stored faces in a computer database in a minute or less.

Advances in face recognition come amid heightened interest in using biometrics such as iris scanners, hand-geometry readers, fingerprint sensors and voice-recognition systems for everyday identification. This is mainly because of a widespread belief that passwords and PINs are easy to compromise. And face recognition is relatively palatable to the general public: It doesn't have the stigma of fingerprinting, the strangeness of sticking your hand into a hand-geometry reader or the spookiness of eyeball reading.

Still, with many people concerned about the erosion of privacy in the computer age, face recognition is making

some people uncomfortable. When the state of Michigan switched to digitized photos, which can be stored in computers, it decided against using face-recognition technology because "the privacy issue is huge," says Rose Jarois, who heads the policy division in the office of Michigan's Secretary of State.

Marc Rotenberg, executive director of the Electronic Privacy Information Center in Washington, D.C., says that ubiquitous security cameras, linked to databases of facial images, "are breathing new life into Orwell's visions of 1984."

Face recognition has spread most quickly as a way to combat fraud. West Virginia uses a face-recognition system to stop people from acquiring different driver's licenses under other people's names. When people claiming they have lost their licenses come to a motor-vehicle center to obtain new ones, the state takes a photo and the computer compares it with the photo that is already in the database. "We've caught a number of people who come in, and when the clerk says, 'There seems to be another photo,' they disappear and leave all their documents," says Dough Thompson, manager of driver licensing for the state.

In Boston, the state welfare agency takes pictures of new applicants and compares them with all 300,000 people in its database to make sure the applicant isn't trying to double-dip by getting a check under another name.

Two years ago, the Los Angeles Sheriff's Department caught a mugger after a sketch was compared with a selection of 30,000 photos in its database. However, Sgt. Bill Conley of the department says Los Angeles still hasn't put many of its 500,000 mug shots in the system, so "we haven't got a lot of success stories to tout."

Visionics Inc., a small Jersey City, NJ, outfit, says its face-recognition system on a powerful PC can compare one

photo with 60 million pictures in a database and select a match. "We've gone a lot further than the human brain, which only needs to recognize a few members of society," says Visionics' chief executive officer, Joseph Atick, who is a former mathematics professor at Rockefeller University.

Visionics was founded by Dr. Atick and two physicists, Norman Redlich and Paul Griffin, from Princeton's Institute of Advanced Studies. Dr. Atick, 35 years old, came to face recognition from a theoretical angle. "We were computational neuroscientists, trying to understand the evolution of human vision," he recalls. "For a species, it's a very competitive domain. One thing we have to perform well from the day we're born to the day we die is recognizing friend and foe."

Dr. Atick and his colleagues were puzzled by how people deal with the amount of visual information they receive. "A human is bombarded by data equivalent to three to four books a second," he says. The scientist concluded we must automatically eliminate redundant information and remember only unique features that are different. That led him to develop computer models of facial characteristics, or landmarks, that would differentiate them from all other faces.

Visionics concluded there are up to 80 landmarks on the whole face; but to make a match, its algorithm needs to find only 14 points that are alike, usually located where the curvature of the face changes.

Once the computer creates a template of the face, it can search a photo database for a match. The computer ignores changeable characteristics like hair color and style or facial expressions, but its focus on the immutable has a major flaw: It can't differentiate between identical twins.

Two other U.S. companies, Miroso Corp., Wellesley, Mass., and Viisage Technology Inc., Littleton, Mass., sell



face-recognition technology. Keith Angell, president of Miros, says face recognition is especially appealing because it can be used to canvass a broad area, often surreptitiously. "In a bad-guy application, face is the only biometrics that can be done covertly, whether in an airport looking for terrorists or a soccer stadium looking for hooligans," Mr. Angell says.

Although casino security won't comment, people familiar with the situation say that a number of casinos in Nevada and Atlantic City are using face-recognition technology to try to spot blackjack card counters when they walk in.

Face-recognition systems can speed up processing of people across borders. Timothy Biggs, section chief of biometrics for Immigration and Naturalization Service, says biometric techniques "are starting to revolutionize our business." He believes that face recognition will eventually replace fingerprints, which are now the main way INS checks identity.

Because a picture can be taken even while people are walking, face recognition could automate passport control. It could also be used to standardize security procedures and speed the passage of travelers through airports, says Brian Wall, director of security services for the International Air Transport Association in Montreal.

In one sign of growing confidence in face recognition, San Francisco's Innoventry Inc., which is 40%-owned by Wells Fargo & Co., is cashing checks at ATM-like devices based on a facial scan. Customers register at a kiosk by picking up a handset and answering a series of questions while their picture is taken. Next time they come with a check, they just enter their Social Security number and the kiosk verifies their identity with a photo. ■

*(William Bulkeley is a staff reporter of The Wall Street Journal. This article appeared in the December 7, 1999 issue of The Wall Street Journal page B-1 and B-4.)*

## Getting Serious About Identity Theft

By: Margaret Mannix

### New federal database tracks this alarming crime.

Victims of identity theft are finally getting some respect – or at least some long-deserved recognition. Last year, when Congress made identity theft a federal crime, it directed the Federal Trade Commission to establish a clearinghouse for identity-theft complaints and assistance. That came on the heels of a General Accounting Office report documenting how widespread identity theft is becoming. The Secret Service, for example, says victims and institutions in its identity-fraud investigations lost \$745 million in 1997, up from \$442 million in 1995.

Identity theft occurs when someone uses your personal information, such as your name, Social Security number, and date of birth, to establish a parallel identity. That allows them to pretend to be you to open bank accounts and apply for loans, for example. The impostors don't pay the bills. Though victims are not liable for charges made on fraudulent accounts, it can be a nightmare to get credit reports cleaned up.

But even with the new clearinghouse, the burden remains on the victims to straighten out the credit mess the imposter has made. The clearinghouse's Web site ([www.consumer.gov/idtheft](http://www.consumer.gov/idtheft)) and the counselors who staff the FTC's toll-free hotline (877-438-4338) will provide advice on what steps to take, such as getting fraud alerts placed on credit reports. "A lot of people don't have a clue," says Elsie Strong, who heads the Victims of Identity Theft support group in Los Angeles, a project

of the California Public Interest Research Group.

**Caller ID.** The FTC will maintain a database of complaints, referring them to law enforcement agencies at the state and federal levels. "Consumers don't have to call us and the Secret Service and the FBI," says Beth Grossman, the the FTC's identity-theft program manager. "We think it's a significant, growing problem," says Joshua Hochberg, chief of the fraud section in the U.S. Department of Justice's criminal division. "I would expect that there will be a significant increase in the number of federal prosecutions."

But the feds typically focus on large-scale scams. That leaves many cases in the hands of local police. Chris Wid-

mer, a detective with the North Charleston, S.C. police, says his department doesn't have the resources to investigate many cases, as suspects are often unknown and located in other

jurisdictions. "If I could, I would put them all in jail," says Widmer, who says all he can do in most instances is file a police report. But that still helps.

A sure sign that a phenomenon has reached critical mass is when marketers swoop in. In September, Travelers Property Casualty Corp. rolled out its Identity Fraud Expense Coverage, which reimburses victims for expenses they incur, such as loan reapplication fees and loss wages. ■

*(This article appeared in the November 1999 edition of the U.S. News & World Report, pg. 88.)*

