The Measure of Man

By: Simson Garfinkel

Computers are getting to know what you look like – perhaps too well.

In 1989, feeling flush with cash from my first book contract, I bought a voiceprint lock for $1,500 and had it installed on the front door of my condominium. The device was the size of a shoe box, with a keypad on the front and a four-digit red LED readout. To get into my house I would simply enter my code (9#) and say my password ("airplane"). A moment later, the door would unlock. Overall, the system worked pretty well, but it wouldn't let me into my house during a loud thunderstorm or, ironically, when an airplane was passing overhead. When I sold the condo, the new owners painted over the voiceprint reader and installed a more familiar, keyhole lock. They weren't quite ready for the technology, and the technology wasn't quite ready for them.

A decade later, computerized biometrics–systems that read your body measurements or patterns such as fingerprints, voiceprints, iris prints, or facial features – have finally come of age. The U.S. Army is building a huge biometric database intended to simplify everything from salary payments to military security. Banks are experimenting with iris scanners as a way to replace ATM cards and numerical pass codes. A prototype cell phone incorporates a thumbprint reader to prevent fraudulent use. And security companies are developing low-cost devices that could provide more privacy for your home PC. As a result, the $60 million commercial biometrics market is expected to grow tenfold in the next three years.

Fingerprints, which are by far the best-established biometric markers, have thoroughly proven their worth in the world of law enforcement. More than a hundred years ago, police in Argentina began recording fingerprints left at a crime scene to identify suspects. The idea quickly spread. Throughout the 20th century, U.S. police departments and the FBI compiled "10-print cards" from suspects and lifted samples of fingerprints from crime scenes. But as these files grew larger and larger they became less and less useful, because searching for a match was manual. By the mid-1980s it would have taken a single worker more than 33 years to search the U.S. Department of Justice's 3,000,000 fingerprint cards for a match according to a 1987 department report.

Computerized fingerprint systems fundamentally changed the rules. As police departments scanned fingerprint cards and latent prints from crime scenes into their computers, the computers rapidly found matches and solved crimes that had been given up as hopeless. In 1985, the first latent fingerprint search on San Francisco's computer turned up the killer of Miriam Slamovich, a World War II concentration camp survivor who had been shot in the throat by a home intruder seven years earlier. The killer was arrested the same day.

Now electronic fingerprinting is catching on in the office. "The biggest applications are the 'log in' process,' says William H. Saito, president and CEO of I/O Software, a California firm that sells software for fingerprint and face recognition systems. Instead of having employees remember dozens of passwords for different computer systems, companies are using biometric systems to implement "single sign-on," Saito says. A worker just sits down at the computer, presses a thumb against a credit-card-size scanner, and the system automatically unlocks the files and applications that person is authorized to use.

"Among the Fortune 1000 companies it is a no-brainer," says Saito. He also sees interest in biometrics spreading to small offices and home-computer users. "We can prevent an application launch – we won't let people launch Quicken, for example, without a fingerprint," he says. A family with a single home computer could use this technology to prevent teenage kids from accessing Mom and Dad's financial records. I/O's software can also control the Web browser, so that younger family members can access only specific Web sites. Eventually, fingerprints might also be used to finalize business transaction – tax payments or home refinancing, for instance – conducted over the Internet. President Clinton recently approved a bill that would make such electronic signatures as legally binding as traditional ones in pen and ink.

Sounds promising, but commercial biometrics has a history of false starts. That's because the systems don't actually identify a person; they merely compare a measurement of the human body with a stored template. If the measurement and the template are similar enough, the comparing software declares the two a match. Early systems sold in the 1980s didn't do very well on these comparisons. They were subject to high numbers of false positives, in which the system erroneously matched a person's measurement with the wrong template, and false negatives, in which the computer failed to identify a real match. Today's systems are far more accurate, thanks to faster computers, but they still make mistakes.

Voiceprint Ids, a staple of science fiction since *Star Trek* in the 1960s haven't found widespread use largely because of technical difficulties. "The inherent problem is that all microphones are not created equal," says Saito. "Ambient noise is another problem, especially if you are outside on a tarmac, inside a client's office, or in a classroom full of kids." Or, in my case, standing in the rain, trying to get the voiceprint lock to open between thunderclaps.

Striations in the eye's iris are a

thousand times more distinctive than the whorls on a finger, so in principle iris prints should be even more reliable than fingerprints. In 1995, the first iris scanners were successfully deployed to provide security for prison doors and bank vaults, says Lou Sassano, vice president of worldwide sales for IriScan, a New Jersey company that holds patents on the technology. Bank United of Texas recently set up three automatic teller machines equipped with IriScan technology in Dallas. "The recognition is so secure you do not have to use either your ATM card or your PIN number," says Vern Stockton, a director at Bank United. Iris recognition adds approximately $5,000 to the overall $15,000 cost of a ATM. Late this year, IriScan will introduce a $200 camera for desktop computers.

Part of the appeal of iris prints is that they require no special action – they can be read without a person's knowledge. Facial recognition is prone to error but is even more stealthy. Viisage Technology, a Massachusetts firm, has developed a system that would allow police to scan a driver after they have stopped a vehicle. Their approach, based on technology developed at the Massachusetts Institute of Technology Media Lab in the early 1990s, would use a hidden camera on the officer's collar to photograph people in the car. Then a pair of radios would transmit the image to the police station, where a computer would run a comparison against a face-recognition database and transmit an alert to the officer if the driver were wanted or dangerous. Another Viisage product, called Hunter, is designed to pick out known terrorists from airport surveillance cameras. More than 50 casinos already use a similar system of hidden video cameras and computers to identify known scam artists and card sharks.

This ability to surreptitiously identify people rings alarm bells for many civil libertarians. Merchants could build a mailing list of every pedestrian who looked with interest in a store window – or deny entrance to suspected shoplifters. Police could use outdoor video cameras to build a list and then question every person who happened to walk in an area after a crime had been committed. A prototype of such a system is being tested in Newham, England.

There are no laws in the United States to regulate the collection or use of biometric information. "Biometrics is one of the most urgent privacy issues," says Marc Rotenberg, director of the Electronic Privacy Information Center. Biometric identifiers could replace social-security numbers and become a kind of "informational flypaper," he says, so that everything about you – your product preferences, credit history, youthful indiscretions – sticks with you for life. Someday you might feel a strange nostalgia for old-fashioned signatures and ATM cards, not to mention lock and keys. ■

(This article was from the Sept. 2000 issue of Discover magazine, pg. 28 – 31.)