

[SHRM Home](#) > [Publications](#) > [HR Magazine](#) > [Articles](#)



March 2003
Vol. 48, No. 3

ARE YOU READY FOR BIOMETRICS?

Devices such as fingerprint scanners may become more common in the workplace.

By Bill Roberts



You might think security systems that use fingerprints or other physical traits for identification belong only at the FBI or the CIA, but some employers have found that the devices can help solve some employee discipline problems as well as protect sensitive data.

Online Feedback

We want your feedback. After reading the column, [click here](#) to fill out a quick, seven-question survey.

For example, the School District of Philadelphia adopted finger scanning to prevent “buddy punching” by some of its 3,000 maintenance workers. Buddy punching is a problem in work settings with ordinary time clocks such as those that use swipe cards or personal identification numbers (PINs). For example, Buddy No. 1 goes home an hour early and gets Buddy No. 2 to punch him out at the correct time. Buddy No. 2 arrives an hour late the next morning, but Buddy No. 1 punches him in at the correct time. Result: The employees stole two hours from the company.

Philadelphia school officials didn’t know how widespread buddy punching was, but they knew it was a problem, says Rich DiCaprio, a now-retired administrator who oversaw the finger-scanning project. Riding herd on the problem, he says, “was very time consuming and costly.”

Time clocks are one of a growing number of workplace applications of biometrics—using physical traits for identification. Traits most often used are fingerprints, and iris, hand or finger geometry. There’s no sea swell here: Biometrics systems are only nibbling away at identification systems that are based on passwords, PINs and swipe cards. But biometrics is clearly no longer limited to secretive government agencies.

The events of Sept. 11, 2001, heightened interest in secure access to offices and facilities in both the public and private sectors and caused an increase in purchases of biometrics systems. Also, the widening use of computer and other electronic networks increases the need to both limit access to networks and ease access for authorized users.

The cost of biometrics systems has dropped, but they can still be initially costlier than swipe card and password systems. However, they can also save money. Dealing with forgotten network passwords and lost smart cards can cost a company a few hundred dollars per user per year, says Trevor Prout, marketing director for the International Biometric Group (IBG), a New York City-based consulting, testing and market research firm. Those costs disappear with biometrics.

A bigger hurdle than cost is the Big Brother connotation associated with using an individual’s physical traits for identification. For example, there is a misperception that the FBI could use corporate identification systems to track average citizens. In fact, that is not true, but that concern is slowing the adoption of biometrics in the workplace.

However, biometrics systems are likely to become more widely used, and it will be HR’s job not only to help administer them but also to educate workers about the limits of these systems as well as their advantages

over other identification systems. For example, while biometrics' perceived threat to privacy concerns workers, it actually can protect them from identity theft, which could occur if a co-worker stole a password or smart card.

Identification Gets Personal

Using human characteristics to identify people is as old as civilization itself. The ancient Egyptians measured height for identification. Ancient China was the first to use fingerprints. Police in Europe and the United States have used fingerprint identification for more than 100 years. In the 1960s, the FBI began to automate it, and by the mid-1970s the agency had installed Automated Fingerprint Identification Systems (AFIS) throughout the United States. Now police around the world use AFIS.

The first biometrics time clock, used in the 1970s, measured the shape of the hand and the length of the fingers, which is called hand- or finger-geometry identification. Iris identification came into play in the 1980s.

By the 1970s, secure facilities for military and government began to use biometrics, as did some civilian operations in the defense and nuclear power industries. In the past decade, as prices have come down, biometrics systems have steadily gained in usage at banks, insurance companies, hospitals and local governments.

"Customers in regulated industries are especially interested," says a spokesperson for SAP AG of Walldorf, Germany.

IBG estimates that the biometrics market will grow from \$500 million a year in 2002 to \$4 billion in 2007. Jennifer Kim, a former IBG senior consultant, says one-fourth of the 2007 industry revenues will fall in the government sector, and a little less than one-fourth will fall in law enforcement. She expects significant growth in financial services and health care—\$700 million and \$400 million markets, respectively, by 2007, she says.

So far, HR professionals haven't been instrumental in biometrics adoption, says Ron Moritz, senior vice president of eTrust Security Solutions for Computer Associates International Inc. of Islandia, N.Y. "Business unit leaders are looking at applications and acknowledging the need for stronger authentication than the traditional password. I don't think HR is driving it."

That may change. By 2007, Kim says, the market for biometrics will include about \$600 million for physical access control systems and about \$900 million for network access control, areas that will impact HR. Some HR departments have asked about biometrics for new e-learning systems, and SAP's learning management product will soon incorporate a biometrics option, a company spokesman says.

Options

Fingerprinting and iris scanning are the most widely used biometrics. There are two kinds of fingerprint technology: In one, the user passes his fingertip over an optical reader; in another, the user presses his fingertip directly onto a computer chip. Finger geometry is still used, especially in situations where fingerprints might be difficult to read due to excessive dirt or calluses. Newer technologies, which have undergone fewer tests and are more expensive than the others, include retina scanning, voice recognition, facial scanning and signature recognition systems.

None of these technologies is 100 percent accurate, says Kim. "But high levels of accuracy are possible, depending on the type of technology you use."

Iris scanning is the most accurate because the iris does not change after infancy, says Kim. It is rare, but two fingerprints can be the same or similar enough to cause problems, and they change with aging. Still, in the relatively small population of a corporate workforce, that is unlikely to present statistically significant problems. Finger geometry's accuracy is also quite high, says Kim.

Iris scanning is used mostly, but not exclusively, for physical access to secure premises. For example, the Federal Aviation Authority uses iris scanning at each desktop PC to control access to its networked executive information system. Generally, however, companies adopting biometrics for network authentication choose fingerprint technology.

Iris scanning is costlier, and there's only one developer, Iridian Technologies Inc. of Moorestown, N.J., Kim says. Fingerprint scanning is less expensive, offers a broader range of products at various prices, and there are several developers. For example, one vendor offers an optical fingerprint scanner that plugs into a desktop PC for as little as \$99.

The Philadelphia school district spent \$1.2 million for 284 finger-geometry time clocks, a server and software to run on its wide area network, says DiCaprio. The system could cover thousands of employees beyond the initial 3,000 if the district decides to expand its use.

Previously, the district used low-tech time cards, which were hard to read and administer. Officials had planned to upgrade to a computer-based swipe card system but opted for biometrics when they determined that swipe cards would be expensive to maintain and replace, says DiCaprio. And the swipe card system would not have alleviated the costly buddy-punching problem.

Privacy Concerns

Once folks get beyond the cost issue, the big problem is psychological. "There's an inherent fear of technology, especially when you see it as potentially dangerous," says Moritz. The big fear is that any fingerprint system is an invasion of privacy and one step toward colluding with the police. But most of the systems sold for commercial use are not capable of that.

The AFIS deployed by the FBI are sophisticated, multimillion-dollar computer networks that capture and store images of actual fingerprints. These images can be shared with other authorities to help identify and link suspects to crimes.

In contrast, most commercial fingerprint technology doesn't store fingerprints. Instead, the technology takes a digital photo of the fingerprint, extracts its unique features, and then turns the information into a mathematical template, which it stores. Each time a worker's fingerprint is scanned, the system takes another photo and converts it to a mathematical template, which it compares with the one on file. The templates consume less storage space, are easier to compare and improve the performance of the system, but they are virtually useless outside the system because you cannot recreate an actual fingerprint from them.

There are a couple of other safeguards, IBG's Prout says. The FBI assures the biometrics community that it does not keep and store fingerprints it receives to do background checks on new employees in certain industries. Also, companies that do those background checks usually work through a clearinghouse, which provides another level of privacy to the individual, he says.

Iris- and finger-geometry databases are also safe. For example, the information stored in an iris scan cannot be converted into an actual iris print.

All that said, companies still use finger geometry, an older technology, because it takes the fingerprint privacy issue off the table, says Kevin Drummond, marketing manager for Accu-time Systems Inc. of Ellington, Conn. The Philadelphia schools bought its biometrics time clocks through a local reseller of the Accu-time technology. "With fingerprint technology, the information we're taking is not FBI-quality information," Drummond says. However, some people don't believe that claim, so Accu-time sells both fingerprint and finger-geometry systems.

Convincing the Users

The Philadelphia school district chose finger geometry to negate privacy concerns, says DiCaprio. Officials also notified the union that they were thinking about a biometrics time clock and invited union representatives to observe the pilot testing. "The union has problems with difficult employees, too," says DiCaprio. "No one gains from workers who try to beat the system."

The district also decided early that maintenance supervisors would go on the clock, although they had not been on the old clock. "We put the supervisors on the system so as not to stigmatize the union members," DiCaprio says. It helped that many of the supervisors had been one-time union members themselves, he says.

DiCaprio met with about 40 groups of workers to discuss the new technology. Besides the FBI fears, the

biggest concern was health related: If a worker who used the system had AIDS or hepatitis, could the next employee contract it from the device? DiCaprio said he assured workers that touching the device was no more dangerous than touching money or a doorknob.

Bill Roberts, technology contributing editor for HR Magazine, is a freelance writer based in Los Altos, Calif., who covers business, technology and management issues.

Reprints and Permissions



Society for Human Resource Management

1800 Duke Street • Alexandria, Virginia 22314 USA

Phone US Only: (800) 283-SHRM

Phone International: +1 (703) 548-3440

TTY/TDD (703) 548-6999

Fax (703) 535-6490

Questions? [Contact SHRM](#)

Careers [Careers @ SHRM](#)

Copyright © 2006, Society for Human Resource Management

[SHRM Privacy Statement](#) | [Your California Privacy Rights](#)

[Terms](#) under which this service is provided to you.