reaction aids detection by copying small fragments of bioagent DNA many thousands of times in a few minutes. The USPS is now evaluating the effectiveness of this and another prototype, from Idaho Technology Inc. (Salt Lake City, Utah) and Lockheed Martin Corp. (Bethesda, Md.).

Of course, all such work is hindered by the fact that the USPS has no significant R&D budget and thus no research tradition. This seriously inhibits the agency's ability to identify, develop, and evaluate solutions. That is changing. This year the U.S. Congress allocated $500 million to the postal service for bioterrorism defense. Of that total, $200 million will go to purchase detection systems for 292 mail facilities. But at least another year will pass before the systems are installed, and the USPS estimates annual operating costs at $100 million. The USPS also plans to retrofit its high-speed sorters with air vacuuming and filtration apparatus, at a cost of $245 million. It is also considering deploying radiation detectors to detect "dirty" radiological bombs.

### Toward smart mail

Stamped letters and packages that enter the postal system through mailboxes—so-called anonymous mail—are thought to present the greatest terrorist threat. About 83 percent of mail, though, comes from commercial mailers who have USPS accounts; that mail carries a bar code and is easily traced to its sender.

In the longer term, Tom Day hopes such "intelligent mail" will grow even more popular. The postal service aims to upgrade its mail-scanning cameras to read two-dimensional bar codes. These would contain more data than current bar codes, including such details as the mail's origin, destination, and type, but would still be printable on regular desktop printers.

Today only mail destined for Congress and the Executive Branch continues to be irradiated. Meanwhile, the Brentwood and Hamilton mail facilities (in Washington, D.C., and Trenton, N.J., respectively), which suffered anthrax casualties, remain closed for decontamination.

Will terrorism once again stay these couriers from the swift completion of their appointed rounds? Only time will tell.

**—Christopher Aston**
Contributing Editor

# Who Goes There?

**High-tech personal identity systems make us more secure than a year ago, but not by much**

**BIOMETRICS** • Just a few years ago, getting to work involved a nod to someone in the building lobby or a wave to an office receptionist. Today, those friendly greetings have been replaced in many offices by smart cards.

Soon the use of smart cards at these sites is expected to make way for biometric identifiers: handprints, fingerprints, eye scans, or face-recognition signatures. On the way to work, too, one's face or car may be scanned or photographed at traffic signals, bank machines, shopping malls, parks, and sidewalks.

The past year has been a busy one for identity systems and biometrics-based security. An initial surge of interest, support, activity, and even funding has given way to harder looks at whether cutting-edge systems, especially for face recognition, are ready for prime time. It turns out they are not. And second thoughts about the potential loss of privacy abound.

A good example—of both the initial interest and the second thoughts—is the creation of national ID cards in the United States, an idea long rejected by citizens and legislators alike. In the weeks after 9/11, many people, including noted Harvard University law professor, civil liberties lawyer, and activist Alan Dershowitz, were newly ready to favor security over privacy. Jumping on the bandwagon, Oracle Corp. CEO Larry Ellison proposed a national ID database—accompanied by an offer to contribute his company's flagship software for free—but the idea struck many as a self-serving, the-razors-are-free-but-the-blades-are-gonna-cost-ya idea, and was rejected.

Nevertheless, standards were soon proposed for state driver's licenses that would be machine-readable and include biometric data and space for other digitized personal data. Corollary proposals calling for states to share information with each other and the federal government would yield licenses that have all the qualities of a national card.

The threats to privacy do not stem just from the government. For example, boarding a subway or shopping at a supermarket has traditionally been a relatively anonymous activity. But, according to one newspaper account, soon after 9/11, an employee at an unnamed U.S. grocery chain supplied law enforcement authorities with customer databases built from preferred-customer-card shopping activity. With standardized smart card driver's licenses containing nongovernmental identification information, it could be even easier to track people through their commercial transactions. What's more, combining hitherto separate identity systems could maximize the potential harm of identity theft.

Many countries already have national IDs in one form or another, and others are adding them. In Japan, an 11-digit numeric code for residents, established in 1999, is the cornerstone of a new, highly controversial, smart card-based ID system, using software from Microsoft and Oracle and hardware from NTT, Fujitsu, Hitachi, IBM Japan, and others. The absence of privacy laws governing the system has provoked rare-for-Japan civil disobedience, and several cities have opted out of the program entirely. Less contentiously, Australia began a trial program to incorporate biometric data in passports.

As methods of identification, however, biometric technologies are still immature, and one, face recognition, has been especially disappointing. In a test this spring of a leading system, that of Jersey City, N.J.–based Visionics Corp. (now merged with Identix Inc., Minnetonka, Minn.), over half the faces in a mock terrorist database used at the Palm Beach (Fla.) International Airport were let through unflagged, while one person in every hundred to pass through the system was falsely labeled "terrorist."

### Older, but not wiser

Older ID and document systems have their own problems. Credit card theft is a perennial, and apparently growing, problem. Even smart credit cards, such as the

American Express Blue card, can be hacked, as two researchers in the United Kingdom recently proved. And in New Jersey, an investigation by the *Bergen County Record* found that, among other things, security failings allow driver's licenses to be issued despite the presentation of inadequate identifying documents. New Jersey was home to at least four of the 11 September hijackers, two of whom reportedly had valid state driver's licenses.

Even with valid documents, problems arise. In recent years, the U.S. Social Security Administration routinely issued tens of thousands of Social Security numbers to noncitizens who presented insufficient or counterfeit identification.

Adding biometric information to driver's licenses may not be enough. Researchers at Yokohama National University in Japan have found they were able to replicate fingerprints with a cheap artificial "skin." They photographed a fingerprint left on a drinking glass, enhanced it with photo-editing software, and then used a photosensitive sheet to transfer it three-dimensionally to a sheet of copper. From there they could move the image onto a highly elastic food-based gelatin. The fingerprint was recognized by a variety of security systems about 80 percent of the time.

That may be more work than is really needed. A recent book by three German researchers told how they defeated a fingerprint scanning system by breathing "gently upon the sensor's surface." They reported that on the screen of the biometrically protected computer, "we were able to see the contours of an old fingerprint slowly reemerge." In all, the team tested 11 biometric security systems and, by a variety of means, defeated each of them.

**–Steven Cherry**
Senior Associate Editor

# Second Site

**Multiple broadcast towers, once thought a waste of money, are now the order of the day**

**BROADCASTING** • Of the thousands who died at the World Trade Center on 9/11, six were on-site broadcast engineers and technicians. They were managing what was then the New York metropolitan area's broadcast hub—the transmitters, the 110-meter mast, and antennas for 10 television stations and two FM radio stations situated atop the North Tower. All broadcasts ceased minutes after impact, and as the city tried to discover what was going on, just one television station reappeared to fill the void.

WCBS-TV was the only station that had transmitters at both the World Trade Center and the Empire State Building. "We had a 37-year-old tube transmitter that saved our bacon when the World Trade Center collapsed," said Robert P. Seidel, vice president of engineering and advanced technology at New York City's CBS Broadcast Group.

Generally stations have backup transmitters and often antennas, but they are always at the same tower. Now all area broadcasters, and to some extent their network parents, want what was once thought unnecessary: having backup antennas and transmitters at more than one tower.

Responding to the attacks, the U.S. Federal Communications Commission (FCC) organized a media security and reliability council to advise it on infrastructure and emergency coordination. The council, populated by such industry heavyweights as Rupert Murdoch, chairman and CEO of News Corp., and Dennis J. FitzSimons, president of Tribune Co., will make recommendations on the need for redundant towers and other infrastructure issues like the need for direct fiber-to-cable head-ends. (While the majority of cable feeds from stations to local cable distributors are fiber, many cable head-ends in the New York area took their input from the over-the-air signal lost in the attacks.)

***A transmitting tower is featured in a proposed World Trade Center design.***

But building new towers across the country will be an uphill struggle, notes Tom Gurley, president of the IEEE Broadcast Technology Society and vice president for technology at the Association for Maximum Service Television Inc. (Washington, D.C.), a local television trade group represented on the FCC council. "The notion of every broadcaster having a redundant tower is a nice idea," says Gurley, "but a huge obstacle in a practical sense."

Apart from the cost, broadcasters must negotiate with zoning authorities and neighbors when siting new towers. And as some who are trying to build new towers for their digital television rollout have found, projects can quickly get hung up on politics. Still, says Gurley, backing by the FCC would help smooth things out at the local level.

"The first thing people do in an emergency is to turn on a local TV or radio station," says Gurley. "9/11 underscored how much [the broadcast infrastructure] is missed when it's not there."

In New York City, most broadcasters' first thought was to get back on the air. Radio and TV stations scrambled to restore their signals by broadcasting from several sites, including the Empire State Building (whose antenna mast was originally built in the 1930s as a mooring for dirigibles). But none of the alternative sites can handle the structural, mechanical, and electrical infrastructure of all the stations at full power. While most New York area broadcasters are sending signals from the Empire State Building at reduced power, a group of TV stations is searching for a site for a new tower.

THE LOWER MANHATTAN DEVELOPMENT CORPORATION