

Keeping a Close

Eye

Officials increasingly turn to camera networks and monitoring devices for public surveillance

By John J. Mountjoy

After the London terrorist attacks in July, law enforcement officials identified the suicide bombers through a network of more than 6,000 cameras in the transit system and on street corners. Although the cameras aided in identifying the perpetrators, they did little to thwart the attackers.

The use of high-tech surveillance devices is an emerging tool in countering threats to public safety. States are increasingly monitoring the public through camera networks similar to ones used in London. In addition, state officials are considering more cutting-edge tracking devices for security.

Keeping a Close Eye

In the United States, cities and states are seeking camera surveillance technology. Several cities have already started using cameras to monitor large crowds. In 2001, at Super Bowl XXXV in Tampa, for example, cameras scanned some 100,000 faces in the crowd.

In 2001,
at Super Bowl
XXXV
in Tampa, for
example, cameras
scanned some
100,000 faces in
the crowd.

Other cities are adopting simple camera networks. Large cities such as New York, Baltimore, Chicago, Detroit and Washington, D.C., have placed cameras in high-traffic areas such as subways, buses, transit stops and popular shopping areas. Even smaller cities such as Durham, N.C., Jersey City, N.J., Athens, Ga. and Chelsea, Mass., use cameras for surveillance.

Homeland security funds have financed the development of the growing number of camera networks. In 2005, the U.S. Department of Homeland Security (DHS) earmarked \$800 million for 50 cities. The Fredonia Group, a national market research firm, projects that the

electronic security products industry for the public and private sectors combined will grow by 8.7 percent each year through 2008 to become a \$15.5 billion a year industry.



States are also upgrading surveillance of their public transportation. Colorado is working to connect more than 200 state highway cameras and other surveillance sources into the state's homeland security "fusion" center, a centralized counterterrorism intelligence and analysis clearinghouse that is increasing in popularity among states.

Surveillance cameras and technology are needed to upgrade the nation's transportation security systems. While the focus remains on air travel, an increasingly important area is mass transit within metropolitan areas and in commuter transportation. Sixteen times more people than those who use domestic airlines use public transportation daily.

However, DHS has spent \$18.1 billion on airline security since Sept. 11 and only \$250 million on transportation security nationwide, according to the American Public Transportation Association (APTA). In 2004, APTA conducted a study of transportation security needs and determined that approximately \$6 billion was needed nationally to strengthen transportation security.

Watching Drivers

States are also using automated traffic tollbooths, which operate off radio frequency identification devices (RFIDs) or "smart tags." RFIDs reduce congestion and employee expenses, while providing greater efficiency. RFIDs are low-powered radio transmitters that read data stored in a transponder, or tag, at distances up to 100 feet away. The private sector uses RFID tags to track assets, manage inventory and authorize payments. In addition, they increasingly serve as electronic keys to everything from automobiles to secure facilities.

The E-ZPass system, available in 10 states—Delaware, Maine, Maryland, Massachusetts, New Hampshire, New Jersey, New York, Pennsylvania, West Virginia and Virginia—is pioneering the high volume use of "smart tags" by motorists. The system, which can be used by participating drivers in any member state, allows vehicles with a displayed "smart tag" to drive through toll stations and have their pre-paid accounts debited for the appropriate toll.

E-ZPass and similar systems are raising concerns about other roles for which the technology might be used. For instance, while the system is currently limited to ticketing speeding offenders in

London is testing a system that uses interconnected "smart" cameras to track drivers over a wide area such as a neighborhood instead of limiting surveillance to a single intersection.

the reduced speed toll zones, they could be used to identify and ticket drivers for speeding over the course of their commute by measuring time over distance and issuing citations automatically. "Automatic tollbooth data has already been used by the courts to prove one's location, either to include or exclude individuals as suspects in criminal cases," said Mark McChesney, Information

WARNING

PREMISES
UNDER
VIDEO SURVEILLANCE

Resources

For more information on state “fusion” centers, see CSG’s 2005 report, *The Impacts of Terrorism on State Law Enforcement*, available at www.csg.org.

Technology Security Chief for the Kentucky Department of Transportation. “It’s only a matter of time before it’s used for other applications.”

London is testing a system that uses interconnected “smart” cameras to track drivers over a wide area such as a neighborhood instead of limiting surveillance to a single intersection. The idea is that by tracking a vehicle over a set course, driving habits such as speeding can be identified and citations automatically issued via the traditional camera feature. As results on the effectiveness of this system are studied, look for this technology in the United States in the next few years.

Another application of RFID tags is used in the United Kingdom: RFIDs are embedded in car license plates. These e-Plates enable a scanner to identify cars. According to the manufacturer, the e-Plate may be scanned by either a handheld portable device or by a stationary roadside device. It can detect dozens of vehicles moving at any speed from a distance of about 100 yards. The e-Plate provides access control to parking areas or restricted access roads, automated tolling, asset tracking, traffic flow monitoring and vehicle compliance with the law. With a 10-year battery, the embedded chip will likely outlast the license plate in which it is stored.

While states are embracing RFID technology, they are also acting to protect and educate consumers about the devices. For instance, bills introduced in Utah and California sought to force retailers to disclose to consumers the presence of RFID tags. Neither bill was enacted. There is strong support from privacy groups for such action.

Opponents, however, contend such laws will increase costs.

North Dakota was the first state to prohibit insurance companies from using data in black boxes to set rates. Insurance companies are using the boxes, now standard in many new American cars, to prove liability in vehicle accidents and to justify rates. Already in use by some rental car companies to track wear and tear and speeding infractions by customers, the black boxes were developed for manufacturers to determine the cause of vehicle problems.

Tracking Travelers and Immigrants

RFID chips are also used to strengthen security and deter the forgery of official documents, such as passports. Similar to the E-ZPass cards and e-Plates, these documents would contain an embedded RFID to store data, ensure authenticity and allow tracking.

Since passage of the REAL ID Act, such technology is being considered for required security upgrades to state issued driver’s licenses.

States and the federal government are also turning to RFIDs and biometrics to track foreigners within our borders and reduce illegal immigration. Biometrics, the study of biological phenomena and statistics, uses human traits such as fingerprints, retinal scans, voice signatures and DNA data sets for identification. Armed with this data, agencies can quickly locate fraudulent documents such as entry visas.

As RFID and other high-tech security features get a great deal of attention, paper is getting a face-lift. Paper contains a unique “fingerprint” of surface imperfections that can be identified, catalogued and used for identification and tracking purposes when combined with a special scanning device.

Detailed in the July 2005 issue of *Nature* magazine, the unique pattern of a sheet of paper remains recognizable even after it is crunched, rolled into a ball, soaked in water, baked at 350 degrees Fahrenheit for 30 minutes, scrubbed with an abrasive cleaning pad or scribbled over with a black marker.

While this does not prevent people from fraudulently obtaining valid documents from the source, such as a motor vehicle department, it does hold the potential for detecting forgeries common on fake entry visas and other immigration and travel documents.

—John J. Mountjoy is director of CSG’s National Center for Interstate Compacts. He may be reached at jmountjoy@csg.org.