Justifying anti-terrorism technologies

Report by Robert N Veeder

BIOMETRICS TECHNOLOGIES have been proposed in the US as a means to counter terrorism. But, asks Robert N Veeder, are we once again letting fear stampede common sense and good policy?

In Washington DC, the National Park Service and District of Columbia government have announced that they are installing video cameras and will begin round-the-clock surveillance at all major monuments on the Mall by October this year. The Mall is the area bounded by the US Capitol to the east and the Lincoln Memorial to the west. Monuments include the Jefferson and Roosevelt memorials, as well as the Washington Monument and others. The intent is to forestall terrorist acts at these monuments in light of a Park Service study which indicated that they are prime symbolic targets for terrorists. The monuments are visited by millions of tourists each year.

The District already has approximately 1,000 video cameras at various locations throughout the city, including streets, schools, and subway stations. It operates a computerised network capable of linking these cameras in response to terrorism alerts issued by the Federal government or when major events such as parades or protests occur. Thus far, the system has not been used to record, only to observe.

The announcement about the surveillance concerns was greeted by a number of wary questions from both the US Congress and civil liberties watchdog organisations such as the American Civil Liberties Union (ACLU), which expressed concern that such monitoring might discourage the traditional use of the Mall for legal demonstrations.

Especially in light of the events of September 11th, video surveillance technologies are being seen as a way to compensate for scarce police resources. According to the *Washington Post*, about "80 per cent of the 19,000 police departments across the country use closed-circuit TV in government buildings and other public areas, according to a 2001 survey." Moreover, airports are also installing video (and even more invasive) devices to screen passengers. For years businesses have used video surveillance to deter shoplifting and employee theft.

> US citizens have historically exhibited a marked sensitivity to privacy threats – especially those promulgated by the government

US PUBLIC IS WARY

Nevertheless, US citizens have historically exhibited a marked sensitivity to privacy threats - especially those promulgated by the government - that target their actual persons. This feeling or awareness is driven in part by rights contained in the US Constitution.

Many years ago, in response to the skyjacking of airplanes to Cuba, the RAND Corporation prepared a study of ways to deter skyjackings. The study considered and discarded the idea of putting metal detectors at the gate areas to detect armed passengers. The authors thought the American people would never stand for such an invasion of their privacy. But ultimately, of course, metal detectors, X-Ray machines and all the other screening devices we now confront when boarding aeroplanes, came to pass because technology seemed to offer a solution and people were willing to make a trade-off in that particular area.

People may to be able to tolerate surveillance that makes them feel safer, (eg. cameras in dimly lit parking lots) or that helps reduce crime, (eg. video monitoring of racks of clothing to detect shoplifters). But, use the technology at street corners to detect red light runners, or on highways to identify speeders, or in clothing store dressing rooms to monitor potential shoplifters, and many question whether the loss of privacy is worth the trade off.

TECHNOLOGY IS NOT FOOLPROOF

As we learned after September 11th, merely having the ability to survey an area such as a boarding gate is insufficient to prevent a particular individual from carrying out some horrific plan. It is interesting to note that in Tampa, Florida, where face recognition technology has been in use, an ACLU report said that "system logs obtained

by the ACLU through Florida's open-records law, show that the system never identified even a single individual contained in the department's database of photographs. And in response to the ACLU's queries about the small number of system logs, the department has acknowledged that the software - originally deployed last June, 2001 - has not been actively used since August."

Part of the problem in using this technology, as John D Woodward, a Senior Policy Analyst with the RAND Corporation pointed out at a recent conference on Privacy and Data Security, is that neither human operators nor computers are very good at facial recognition on the fly. They are much better when starting from a known point, ie. if I already know what you look like, I have a much better chance of finding your face among the crowd. This suggests that databases containing photographs of muggers, robbers, prostitutes, terrorists, and the like, need images of a high quality to be useful. Unfortunately, too often, photos are shot under less than ideal lighting, with less than first class equipment and when subjects are looking away from the camera or concealed under hats or scarves. This suggests that general face checking technologies are unlikely (as Tampa learned) to be particularly effective in identifying particular individuals.

Fixing the glitches

To overcome some of these problems, Woodward suggests using face recognition with existing processes in order to populate databases with high quality images. To do this, one must control the environment where the image capture occurs, eg. at embassies and consulates where persons are applying for visas; or at US entry and exit ports. To assemble a watch list, Woodward suggests using existing intelligence and law enforcement resources, including mug shots of criminal suspects. Woodward would add so-called open sources to the mix – high quality video and still photographs from the media, for example.

With a database of high quality images, automation processes can be used to serve up possible hits to a human operator from a sea of surveyed images, rather than having an operator sit in front of a screen, hoping to find a face that matches some dimly remembered characteristics.

That is the way it could work, in any case, and maybe it would prevent a future Mohammed Atta from boarding a jumbo jet and flying it into the Capitol. But, we would have to know what he looked like, what his affiliation was, and what he was planning.

Clear policies needed

Returning to Washington DC and its monument watch, when the Park Service testified before the US Congress on its surveillance plan, its spokesman, John G Parsons, acknowledged that there were no existing standards and policies for who would have access to any data developed, how they would be used, with whom they would be shared, how long they would be kept, and whether there would be penalties for misuse of the data. Parsons promised that written standards and policies would be forthcoming.

But isn't it frightening and typical that the use of such powerful and privacy invasive technology would proceed without a clear roadmap?

Robert N Veeder is Director of US-based The Privacy Advocates.

For more information on biometrics technology and terrorism, see PL&B International, Feb 2002, p.11.

Air travel security initiative unveiled

By Alan Pedersen

A trial scheme has been launched that is intended to improve airport security through the use of identity verification technology. The scheme uses smart cards containing biometrics and digital certificate technology enabling air operators to provide a secure way to process frequent air travellers at check-in and boarding stages.

The s-Travel (secure-travel) project is a joint initiative by the International Air Transport Association (IATA) and SITA, a provider of global information and telecommunications solutions to the air travel industry. The two organisations will work together to develop global industry standards, ensuring that all technologies will be interoperable with airport infrastructures.

In a press statement, IATA Director General and CEO Pierre J. Jeanniot, said: "Strict procedures need to be followed to ensure the proper authentication of individuals, and IATA's participation in this initiative will involve defining the optimum enrolment procedures and processes. This will contribute to the definition of global standards that will help secure the air transportation system and improve passenger confidence."

Later this year, the project will be trailed by the European Commission and Swiss Office for Education and Science - who have also provided funding for the project - with a view to implementing the scheme on a global scale.

For more information:
Karl Moore, SITA, Tel: +44 208 757 8024,
e-mail: karl.moore@sita.int

Tim Goodyear, IATA, Tel: +41 22 799 2965,
e-mail: goodyeart@iata.org

The two organisations have a joint website at: www.digicert.org