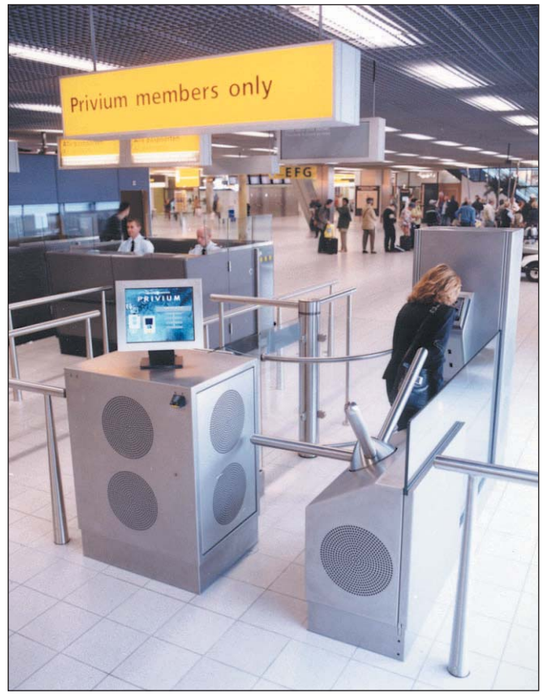
# future focus

**Iris scanners, face-recognition software and fingerprint pads could make signatures and passwords obsolete in the not-too-distant future. Paul Rincon delves into the world of biometrics to examine what this technology will mean for our privacy and rights**

In the shaky aftermath of 11 September, media commentators everywhere went on talk shows to proclaim that the world had changed forever. However, their opinions looked to be informed more by the mind-bending hysteria surrounding events than cold, hard facts. Amid the exaggeration and conjecture, though, this statement becomes more poignant every day. The clash of ideologies, known as the war on terror, hasn't brought about the end of civilisation as we know it, but it will affect our lives in subtle and, some argue, insidious ways.




## Physical identity

Technology is now at the forefront of this new order and biometrics could have the biggest impact. For those who have been living in a bunker for a decade, this is a security method that identifies people by their unique physical features. Biometric security is being touted as the ultimate replacement for passport photos, signatures and fingerprints and, if you believe its exponents, will make our lives more secure.

Regarded as the most accurate form of biometric authentication, iris scanners are becoming increasingly popular as an option for next-generation security. Iris-recognition devices work by scanning an image of a person's iris – the coloured part of the eye – and turning it into a geometric map of over 244 flecks and marks that are unique to that person.

## Seeing is believing

This security method has found a natural home in airports, the institutions placed under most scrutiny following the terrorist attacks in America. Though the scheme was mooted long before 11 September, Heathrow airport is testing an iris scanner with frequent international flyers, allowing them to bypass immigration without the use of a passport.

However, Simon Davies, director of Privacy International, thinks biometric technology is not effective in preventing crime and feels it poses an unprecedented threat to civil liberties. "It [iris scanning] is wildly inaccurate and cannot be relied upon to provide safety for passengers," says Davies. "It is technology in search of a purpose," he adds, suggesting that the money would be better spent on wage hikes for underpaid airport security staff.

The Heathrow scheme is a joint programme between BAA, British Airways, Virgin and the UK Immigration Authority. Invitations to apply for the six-month trial were sent out in January, but as yet the programme has no fixed start date.

Travellers accepted on the scheme will have their irises scanned and the data stored in a database. Passengers flying into Heathrow will be able to present themselves at an iris scanner and, if the data from their iris matches that stored in the database, they can proceed to arrivals. Heathrow says the process of recognition can take as little as two seconds.

## The Dutch look lively

A similar program called the Privium scheme is already under way in the Netherlands at Amsterdam's Schiphol airport. From December 2001, frequent flyers have been able to use an iris scanner to check in their luggage, bypassing manual passport checks.

Privium passengers also have to enrol, but their data is stored on a chip in a smartcard rather than a database. When Privium passengers check in their luggage, they insert their card into a reader which checks its validity. They are then let through a turnstile to the iris scanner.

If their iris geometry matches the data stored on their card, the passenger is allowed through a revolving door to pick up their luggage and head for the departure lounge. If the data does not match, the passenger is directed through another door to the Dutch Border Police counter for a passport check. The Schiphol group, which operates the airport, says the whole process takes 15 seconds to complete.

Like the trial at Heathrow, the Privium pilot scheme was already mooted before 11 September. But a spokeswoman for the Schiphol Group, said plans to make all Schiphol staff use iris scanners at entry points to restricted areas from mid-2002 were a direct result of the attacks in America.





↙→ Iris-recognition devices could make check-in quicker and increase the security at airports, however many experts question the reliability of these scanners

## Sight unseen

Biometric technology is by no means perfect, though. Depending on how it is tested, recognition rates for iris recognition devices vary from 70 to 100 percent. Iris scanners can issue false acceptances to people whose irises do not match the information stored in a database and false rejections of those who do.

But Ed White, marketing director for TSSI, a UK-based manufacturer of biometric systems, dismisses recognition rates as meaningless. Instead he suggests the most dangerous failing could be the initial enrolment process, where applicants could obtain smartcards with false documents. White claims that, provided people co-operate with the machine, biometric technologies are the most secure and accurate means of security at our disposal.

> "These technologies are an important deterrent and don't interfere with people's civil liberties. Most cards don't store any data that's meaningful in terms of people's privacy"
>
> **Ed White, marketing director, TSSI**

"All biometric systems irrefutably match an individual with a document," says White.

However, Davies points out that biometric security will do nothing to stop first-time criminals who are intent on bypassing security measures. He points to the fact that the hijackers who carried out the 11 September attacks were not known to the authorities as terrorists before that date.

"There's no such thing as absolute security, but this is a huge step up," counters White. "These technologies are an important deterrent and don't interfere with people's civil liberties. Most cards don't store any data that's meaningful in terms of people's privacy," he adds.

## Keeping an eye on you

According to privacy campaigners, iris scanners are just the tip of the iceberg. Barry Schlossberg, founder of US info-security consultant Snetcorp, thinks one of the biggest practical threats to civil liberties might come from less accurate face-recognition technology. Face recognition works by taking a photo or video image of a person and converting it into an equation that describes the unique geometric characteristics of that person's face. Software can then make a mathematical comparison between these images and those in an existing database of criminals or terrorists.

But Schlossberg contends that, as biometric data from the general public becomes available to the authorities, tracking a person's movements from place to place will become easier than ever.

## Who's watching who?

Schlossberg claims that the police or secret services could effectively use the technology to single out any individual on a closed-circuit camera, identify them through face recognition and track their movements through the network of CCTV cameras spread across our urban centres. "Face recognition can easily be abused," he says, "For example, what if you're a political dissenter? You can't assume what a government will elect to use this for."

At the time of writing, Home Secretary David Blunkett is attempting to pass his controversial Antiterrorism Crime and Security Bill which will allow far-reaching powers to detain individuals suspected of terrorism. The debate ultimately comes down to what freedoms we'll have to sacrifice to allow governments to protect our security, and technology is a key issue. "The problem with the kind of technology we're talking about is that you're guilty until proven innocent," says Schlossberg.

Schlossberg thinks a future where constant surveillance is the norm is inevitable: "Nothing can stop this now. We're dealing with governments and big business here," he says, "and once you've lost your rights there's no getting them back." ■

More futurama can be found in our Special reports section at www.pcadvisor.co.uk/registered