



Some technical problems with Identity Cards

Price
30p

Government proposals

In November 2004 the Government published a bill to introduce identity cards (ICs). ICs would contain photograph, name, address, gender, date of birth, possibly 'right to work' (or not), and also a microchip containing 'biometric' descriptions of face, iris and/or one or more fingerprints. Signatures can be forged, pin numbers noted and documents obtained fraudulently but if an iris scan of a person in front of you checks against the card he or she is carrying one should be able to assume with great confidence that he or she is the correct owner. Furthermore any information the card contains or is linked to should also be correct. Faked passports, as used by the perpetrators of the '9/11' atrocity, will be a thing of the past. That, at any rate, is the theory.

Thus from October 2006 all new UK passports contain a chip which includes the simplest biometric data - a digitized face photo. From 2010, anyone applying for a passport (new or renewed) will also be issued with an IC and citizens may voluntarily apply for one. Government says up to 80% will apply for a card though, given the cost, this seems optimistic. If Labour are re-elected they plan a parliamentary vote to decide if ICs should be compulsory. From 2008, however, all foreign nationals resident in the country should have ICs.

11 of the 15 pre-expansion EU countries and many others have some form of IC. They are compulsory in Germany but not in France. The data held differs. Most hold the first 5 of the items listed in the first paragraph but Italy's, for example, includes marital status and profession; Germany's height and eye colour; Korea's military record; Malaysia's religion, ethnicity and physical characteristics. In the UK the 5 basic items are held on both passports and driving licences and both are commonly used to confirm identity. UK citizens carried ICs from the 2nd World War until 1952. In the EU ICs are used to open bank accounts, claim benefits, and cross borders.

Why the concerns?

A major cause lies in the development of modern computers and communications. During the war, data was written down and kept on paper records. The clerical hassle involved limited what was worth recording and copying and defeated all but the most determined attempts to cross reference data. Computers make ICs more useful - and more intrusive. The Government would like a national database. Each citizen

would have a unique reference number and the police, Government Departments, Inland Revenue, Immigration Authorities and Intelligence Services would, in theory, all be able to access all the data. Even though computers have been in widespread use for 30 years, personal data is still fragmented and its use (theoretically) restricted to specific purposes. The Inland Revenue, for example, can not access criminal records. Once a unique reference number is established all data, including medical and financial records, could be cross referenced.

This gives rise to two particular concerns: first the risk of error which could have devastating consequences, for example locking someone on income support out of that and other benefits. Second the risk of illicit use of data. It is claimed 1% of employees are prepared to sell confidential information for money.

ICs are intended to deter dishonesty: to prevent people doing what they should not do, for example claiming benefits or being in the wrong place. At one time it was suggested ICs could exclude hooligans from football grounds. One claimed advantage of ICs is that it will be easier to catch illegal immigrants. However most illegals exist in the black economy making no claims on the state. They would only be caught if (a) carrying cards was compulsory and (b) the police made frequent checks on everyone or at least target groups, inevitably predominantly young, coloured males.

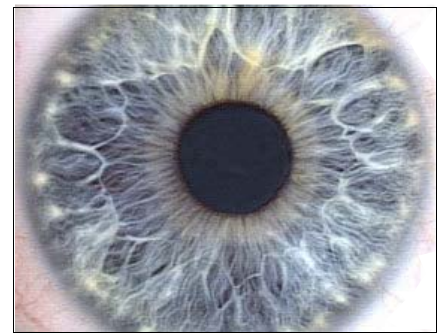


Fig 2. Iris, showing complex mesh like structure

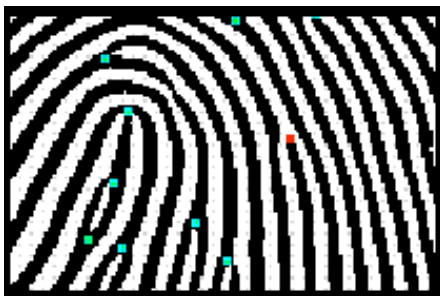


Fig 1. Partial fingerprint showing several bifurcations and one ridge end

Doubts about the technology

In truth the civil liberty arguments may become irrelevant because there is still no certainty the technology will work or work in an acceptable way at a realistic cost. Using data protocols agreed through the International Civil Aviation Organisation (ICAO) the Americans and 27 other so called 'visa waiving' countries including the UK have 'machine readable' passports which have a chip a half centimetre square holding all the printed information on the passport's back page plus a digitized photo. The data is encrypted and read via a radio signal within 2 centimetres (cm) distance (though apparently reading distances up to 30 cm have been achieved which makes them less secure.) The technology is similar to that tried by Wal Mart and Tesco at their checkouts. The 'chip' is read at passport control and the face either shown on a screen for a visual check or scanned for a computer match.

An ALDES Briefing Note

January 2008

This note has been written for ALDES by Richard Balmer. It should be factually correct but any opinions are the authors' alone. If you see errors or have comments contact Richard Balmer at 79, Links Drive, Solihull, B91 2DJ, email richard_balmer@blueyonder.co.uk

Unhappily facial recognition by individuals is poor and, *even under ideal conditions using machines*, is not 100%. In the real world faces age. Men grow and shave their facial hair, women employ makeup. A photo taken in one light looks different to another and can be off centre. The ICAO's *target* accuracy is only 98%. Currently 95% is considered good and some claim there can be 20% or more false negatives and positives.

Consider the consequences at Heathrow on a busy day with 200,000 passengers arriving. A 5% failure rate would mean 10,000 irritated mostly 'legal' people, some with spouses and others with children, being led away for further checks and interrogation. Stories will go from dinner table to the press, the new dawn of biometrics be set back, and the engineering profession take another hammering. Worse if, as Philip Ross¹ says, the system fails every 3rd gentleman with a beard or woman with a head scarf, there will be claims of racial or religious discrimination. Passport officers could lose confidence in the system and start waving both deserving and undeserving cases through. It is one thing to monitor a packet of socks from shelf to check out, but socks aren't self propelled or intelligent and don't need to shave, and even this simple supermarket system is struggling to succeed. Currently relying on facial biometrics looks a poor option.

Fingerprint technology

Fingerprinting and iris recognition data, which can be included in the ICAO passports and is proposed for the UK's ICs, is more promising. Evolution has caused the skin on the hands to be corrugated to increase friction and improve grip. Body cooling (perspiration) leaves a thin film of 99% water and 1% salt on the skin. A touched surface dries leaving a residue of salt. Every fingerprint is unique in shape and, though it expands in size through childhood, remains the same through life, though imperfections such as cracking creep in with old age.

Fingerprint matching systems differ but basically data is collected either by placing a finger on a surface, scanning it and recording the height to the actual skin on an 8 bit gray scale at a definition of about 500 dots per inch, or by pressing the finger down and recording the 'ridges' of the print. The second is simpler, quicker and usually preferred.

In either case the computer ends up with a graphical plot of the print which is then interrogated for features such as bifurcations, ridge endings, 'islands' and 'lakes' of which there may be 150 on one print (see Fig. 1). The co-ordinates and type of feature are then recorded and can be matched. Detail can go right down to individual pores. The amount of data stored depends on use and importance. A company using fingerprint passwords to access computers for example might be content with a 1 in 1000 error rate and so use only a few of the available points. Forensic prints need to be more precise and data files may be 250 kb or even more in size. This, of course, has a knock on effect on system capacity, scanning time, 'usability' and, of course, cost.

The National Physics Laboratory (NPL) considers a good fingerprinting system would only make one error in 100,000 using a single finger. Fingers must, of course, be clean of all dust, grease etc and this can not be guaranteed.

Iris recognition

Irises are also unique and remain unchanged after the colour changes in the early months of life. Iris patterns in fact are even more varied than fingerprints. Irises are better protected from injury and scans don't require actual contact. The iris is photographed in monochrome and searching routines locate the external rim of the iris and the area of the pupil. The

computer 'cuts' the image into radial slivers of 2° or 3° angle each and sub-divides each sliver into sections of different radii. The average 'greyness' of each piece is measured and, using clever statistics developed by Dr John Daugman at Cambridge University, recorded as a chain of data only 512 bytes long. The small file size means that 100,000 iris codes can be scanned per second. Daugman's system was used first in the United Arab Emirates for frequent fliers, and is now installed at Heathrow, Gatwick, Manchester and Birmingham airports with some 150,000 enrolled.

Usability

Both fingerprint and iris recognition would satisfy the 'usability' criteria (although, apparently 18 people per million do not have irises and some have an eye condition where the iris will not remain still) but there is another technical problem. The NPL estimates that iris recognition technology is 10 times (1 in 10⁶) better than fingerprinting. Even so if the UK database holds, say, 50 million records it will come up with 50 matches (it would be 500 with fingerprints) when a new citizen applies for his or her card. This will require bothersome further investigation and cost. The NPL has recommended that iris recognition systems should use both eyes and a fingerprint system at least 4 fingers, preferably all 10. This would virtually eliminate errors and fraud but will require more time, machine capacity and, again, more cost.

Possession is not enough

This leads to the next, crucial, point. *Possessing a card does not mean it is yours*. There is no point having biometric data stored on the card if one then relies on the low tech matching of an individual's face with a fuzzy photograph on the card itself. Fraudsters would simply steal cards and find one with a rough match. One has to have iris or fingerprint readers in *all* benefit offices, police stations, banks and so on to *check* that the individual is the proper owner of the card. There will be a huge charge for this not just to government but councils, banks and others in the private sector. Furthermore, there are simple administrative problems to overcome. The 'system' must be certain the *proper* card holder is requesting a change of address, say, and that a replacement for a stolen, lost or damaged card will actually reach the right person.

The 4 main conclusions

1. ICs alone will do little to reduce illegal immigration unless the police carry out extensive checks.
2. The error rate for facial recognition systems appears too poor for it to gain public acceptance. Without good PR, it could bring biometrics and practitioners into disrepute.
3. Fingerprint and iris recognition systems could succeed but there is great danger the cost will be very high and outweigh the benefits.
4. The potential for creating another expensive 'white elephant' IT system is very high. Given the concern and opposition any sensible government would review its plans and seek independent advice, especially from the engineering institutions most involved. These could advise (a) on the best option if there is one and (b) whether to proceed at all.

Much material for this note has been drawn from the following 2 articles:

1. "Passport to Nowhere" by Philip E. Ross, *Institute of Electrical and Electronic Engineers, Spectrum Online 2.2.05* and
 2. "Safety in Numbers" by Roger Dettmer, *Institution of Electrical Engineers Review Nov 2004*
-