Briefing Paper 11.2

Migration Watch UK

Assuring Identity - a new approach

Summary This paper describes an approach to identity cards which has the following key features:

- No compulsion to acquire a card
- No compulsion to carry a card
- Payment made to those Registering
- Disincentives for those not Registering

This approach maintains all the benefits associated with having identity cards, but avoids those aspects that give rise to objections. The initial estimates are that it will take 8 years to complete the task of Registering the entire population at a cost of some £10 billion, and £500 million per annum thereafter to maintain the system.

Background There have been a number of calls over the years for identity cards to be issued to UK residents as an aid to law enforcement and to try and reduce fraudulent claims on the Social Security system. Recently the perception that the State has lost control over illegal entry and "overstaying" has caused a revival of interest in the subject. Counter arguments are normally on general grounds of liberty, and reference is often made to the hated "pass laws" that existed in South Africa. Recent proposals have included charging fairly substantial sums for such a card, and there is already talk of a "boycott" which reminds one of the Poll Tax saga. Counter-spin has re-dubbed the card as "the entitlement card" without dealing with the objections raised.

Existing Identity Systems Each UK resident uses various forms of identity almost on a daily basis. People working in larger Companies or Government are routinely required to have a photo-id card, which may double as a swipe card for access to premises or systems. Often people have a photo-id and a swipe card(s). It should be observed that the need to carry such cards has never been seen as an infringement of liberty, and that no-one is ever asked to pay for one. It is up to each card-issuer to validate the card-holder's identity in his own manner. People also have National Insurance (NI) numbers, which are used as the index in a number of UK Government systems, but by no means all or even most. There are some 20 million more NI numbers than people, and whilst this difference has been explained away in a variety of ingenious ways, there can be no doubt that the system is badly compromised. There is no way of confirming that the person claiming to be so-and-so really is that person from the NI system as no photograph or biometric data is kept. This is why one sees prosecutions for DSS fraud where one person may have dozens of identities. Other identity-based Applications include the DVLA driver licensing system, which now has a photo-card element, and the Passport system. The latter two are the nearest we have to a National ID system although both are "optional" in terms of either owning or carrying one. Something over 50% of the population hold either a Passport or a Driver's License.

Individuals commonly carry a number of credit, debit and discount cards, all working to different standards. Some do carry photos. However, due to a number of pressures, including those from the FSA, individuals are now commonly also required to produce Utility Bills and the like to "prove" their identity. As such documents are very easy to forge, how much better to have a single, central and secure system?

A National Personnel File All Companies and Government Departments have some form of personnel file for their employees. Indeed is a legal requirement to have one. Many, perhaps most, people find it astonishing that the State does not have a similar file of its citizens. The starting point of this proposal is for the creation of the National Personnel File. The "personnel number" could be used widely, both by Business and by Government Departments such as the DVLA and IR. The advantages of this are obvious. One example would be that if someone married and changed their name, then all the relevant Government records could be updated from one transaction. The corollary is that the new system must have security as its prime design criterion. As no existing systems are capable of positively identifying a person, it will be necessary to develop new ones from scratch.

The personnel file will include the obvious items (name, date of birth, place of birth etc), 2 digitised pictures (front and side) and such other biometric data as may be economic to collect. People often mention DNA, fingerprints and Iris patterns as suitable candidates for storing on such a database and all have their plus and minus points. It is not practical (in both time and cost terms) to analyse and store more than a tiny fraction of a humans DNA. Automated fingerprint systems are not 100% accurate and there are already Internet sites dealing with Iris counterfeiting. No doubt over time the economics and reliability of the various methods will improve, and new ones will be invented, but in the meantime it would be wise to collect as much data as possible, even if it is not practical to utilise it all at the start of operations. With this system, security is paramount, as people will try and "break the system" from day 1.

Outline Design The Master Personnel Database will exist twice, at 2 secure locations. Each copy of the Master Database will have no contact with the outside world by any telecommunications facility, so that "hacking" will be impossible. Staff will be positively vetted and all updating will be done via checked "transaction files" which will be physically delivered on secure media or transmitted in encrypted form using various security techniques to an independent system offline from the Master. After independent updating the two systems will be checked against each other using "hashing" techniques so that any "subverting" would need to be performed on both systems at the same time. The approach at the centre is similar to that of very secure financial systems. By utilising read-only copies for operational use we get the ease-of-use associated with the Internet by implementing a series if Intranets. It should be added that using Internet technology does not imply public Internet access.

All Operational access to the database will actually be to multiple copies or subsets of the Master which will be refreshed each day from the "Master". These copies will be read-only databases. Access to these copies will use Internet Standards, so that cheap, off-the-shelf devices can be used to store and access them. The normal Operational Subset for Uniformed Police use might include the Photos and basic (name etc) data, whereas CID may also want (say) fingerprint data and Forensic Labs might need DNA data. The point is that many of these Operation Subsets can be created and then integrated relatively easily into existing systems. Thus the Police could, if they wish, have a link to/from existing Police National Computer systems so that a wanted person might be identified. This architecture avoids any "Big Brother" charge, and allows rapid local utilisation of the relevant data within the existing local security protocols.

Most important of all, such a design makes it unnecessary to actually carry an identity card, as the information would be online to authorised personnel. If, for example, a uniformed policeman required someone to identify themselves, and they had no id-card with them, then simple inputting of name and date of birth is likely to produce one "hit" and a picture. This could be done on a modern mobile phone or similar using simple internet browser technology. At Social Security offices, access would be via a standard PC using standard software. In the event of multiple "hits", then "tie breakers" could be used, including the "mothers maiden name" favoured by the Credit Card Companies. In fact the process of identifying oneself would be very similar to that employed by Credit Card Companies when dealing with a telephone query, but with the addition of a picture. If a card was produced and the Policeman suspected that he was dealing with a forgery, then the simple input of the personnel number would deliver a picture and other data for comparison. This would make the forging of cards fairly pointless, unless one could also subvert both the Master Databases.

Implementation Considerations Computer systems are only as good as the quality of the data they use - garbage in, garbage out. Collection and input of the primary data (name, image, fingerprints etc) and examination of documents required (passport, Birth Certificate etc) must be done at reasonably secure locations and conducted by trusted and experienced staff face-to-face with the applicant. As it is to be expected that determined efforts will be made to subvert this aspect of the system, cross checks must be made to other Government systems as appropriate and perhaps to commercial organisations such as Experian to check on the Register of Voters.

As the main objectives of this system are to assist is controlling crime, identity fraud and illegal residency, it would be sensible to implement this system first for those groups most likely to fall into these categories. The suggested implementation sequence is:

1. Those claiming asylum (at the point of claiming)
2. Those who have claimed asylum and are awaiting a verdict
3. Those claiming benefits for the first time
4. Those already claiming benefits
5. The rest of the population, possibly in alphabetic sequence

Illegal Immigrants
A major issue would be how to deal with those illegally in this country. The Home Secretary recently admitted that he "hadn't a clue" how many there were. Where there were compassionate grounds not to deport, the person could be issued with an ID card valid for only a limited period and subject to review. In any event the ability to positively identify such people is a prerequisite to the effective management of the problem.

Charging and Compulsion It has been suggested that people be charged quite substantial sums for Registering. As great benefits will be felt by the nation as a whole over many years, and as charging will act as a focus for dissent as with the "Poll Tax" such a policy would be myopic. The Registration process will inconvenience honest people and the State will gain hugely. People should be rewarded for Registering - perhaps £50 per person.

It has been assumed by commentators that Registration would be compulsory - but why? It matters not if a legal resident and would-be martyr declines to Register. They would, after a grace period, simply cease to qualify for benefits.

Furthermore, commercial organisations that currently insist on customers producing Utility Bills etc are likely instead to require production of an identity card.

This combination of pressures will eventually ensure very high Registration percentages without compulsion.

Timetable The UK Government has a very poor record implementing computer systems on time and to budget. Further, this system requires sophisticated and secure clerical processing and bulk processing of biometric data. Security is paramount, but one might also argue that time is of the essence. If one were freed from the bureaucratic process and good leaders and managers appointed with a clear brief and appropriate powers and budgets, how long might implementation take?

1. Recruitment and key personnel and Creation of outline plan and design, including biometric definitions and clerical systems - 1 year
2. Detailed design of database, data-collection, clerical and security processes - 1 year
3. Implementation of "mark 1" system including testing and clerical training - 1 year
4. Input of population of (say) 60,000,000 people - 5 years

Items 1 through 3 above do have some overlap, so all of item 1 need not be complete before item 2 is started, and so on. On this basis the timetable might be reduced somewhat. In addition, during item 1 some prioritising may occur for political reasons. By the same token, politics will cause unforeseen difficulties. The earliest possible time to commence operations would be 2.5 years from the starting date, and in the real world, 3 years is ambitious enough. Thus it will take 8 years to fully implement the system from the starting date.

A functional system for recording Asylum Seekers details could be implemented much more quickly. This might be restricted to one location, and would have to deal with much lower volumes. A basic system could be implemented in less than a year. The Temporary system would continue until the full system is implemented and would also have the benefit of providing practical operational experience that could result in improvements to the main system.

Costs The vast bulk of the costs will be in the collection and verifying of the personnel data. There will also be technology costs such as those associated with storing the duplexed Master databases. If one assumes 1 megabyte of data per person, (60 terrabytes total) the cost should not exceed £5 million and pro-rata. Thus 10 megabytes per person would cost less than £50 million to store. These prices are declining all the time and technology costs can be safely ignored as an important factor.

To collect and verify the personnel data it will be a requirement for all applicants (with obvious exceptions such as the bed-bound) to attend a local centre, where digital photographs would be taken, iris scans and fingerprints taken, documents inspected, and any questions asked. Obviously many cases will be simple, and others very complex. Taking a view of the time needed/person, and assuming that one person can on average process 4 applicants/day, then some 15,000 people would be required to complete the task in 5 years. For a "classic" nuclear family of 4 passport-holders, this may seem easy, but firstly, not everyone falls into that category, and secondly there are significant "back office" tasks to perform with (say) fingerprints and iris scans. This estimate should be treated with some caution, and one of the outputs of the first year's work will be a more accurate estimate. At this stage it would be prudent to treat this estimate as a minimum, and budget for "up to 25,000 people" for 5 years, and to maintain the database thereafter, perhaps 10,000 people permanently. The maintenance would include births, deaths and marriages, new immigrants and new photographs as babies grow up to become adults and other changes to the basic data. If such a reliable data source existed, then significant savings should accrue to other Government departments over time.

During the "take-on" phase (25,000 people for 5 years) I have assumed a cost-of-employment of £50,000 pp/pa, to include office space, furniture, PC, networking and so on. This gives a set-up cost of £1.25 billion pa for 5 years, or £6.25 billion in total, including collecting DNA, Iris and fingerprint data but only storing that data on the database very selectively. The £50 pp bounty would cost a further £3 billion. Allowing for development costs and additional infrastructure technology, the cost up to conclusion of the take-on is estimated to be in the order of £10 Billion over 8 years.

The maintenance phase on the same basis would cost £500 million per annum. As DVLA costs some £300 million pa, this estimate is within common-sense bounds.

This investment would give a secure system with digitised photographs and verified personal data. However whilst fingerprints, DNA samples and iris images can and should be collected at this stage, and the cost of so doing is included, it is unclear what should be done with them. All three technologies have significant uses and limitations. To "sequence" a small part of DNA to look for specific components can cost as little as $50 per sample in bulk. But to process 12 million samples per annum requires a new industry. The security aspects, the need to keep a separate physical sample for possible full analysis and the need to sequence sufficient base-pairs to ensure uniqueness probably means an extra cost of at least £50 pp, or £3 billion in total. Iris images are probably unique but the iris "readers" are only 95% accurate. Imagine one person in twenty being detained at Gatwick in August. In addition, the whole set of iris technologies are currently too expensive to be a practical universal solution. Similar considerations apply to fingerprinting. The common-sense compromise would be to **collect** such data from each applicant, but to process it (for storage on the master database) very selectively. As technologies advance, it may well become economical to process more and more over time.

In addition there will be costs incurred for storing the Operational subsets and accessing them for various applications. It is suggested that these are looked at as separate business cases each on its own merits. Due to the architecture of the system, in many cases these new facilities will be able to be linked in to existing systems at minimal cost.

The Identity Card With the definitive record being held centrally, the actual card is more of a convenience. It should not be necessary to have more elaborate mechanisms than are employed by the more advanced credit-card Companies, or ski-resorts such as Verbier. Here a transponder in the lift-pass signals the expiry date to the turnstile-controlling computer and transmits the image of the skier to a monitor screen, all without being removed from the skier's pocket. Because the physical card is only a convenience and not the "true record", lost cards can easily be cancelled and re-issued.

The Author This paper was prepared by Nigel Foster of Great Communications Limited. He designed and implemented some of the most complex computer applications then in existence until 1974. He then joined IBM and in the 1980s he designed, sold and implemented the new computer systems that transformed DVLA, on time and within budget. During the 1990s Nigel was an Internet pioneer, including co-founding the worlds first Internet Café (Cyberia) in 1994. He now Directs an innovative software and services Company in London (which has no connection with identity cards).