Security risks transform plans for UK ID database

Laura Linkomies

While Australia has just introduced legislation for the Access Card into federal Parliament, the UK ID card scheme is in full swing. In latest developments, the UK Government has scrapped plans for one big database to create the National Identity Register, and will instead base the ID card scheme on three existing IT networks. Laura Linkomies looks at how the identity scheme is evolving.

The UK Home Office's original plan was to build a single database for the ID card scheme. Creating a brand new database was hoped to reduce the risk of having false information on individuals. The UK Government has now, however, decided to opt for using existing databases to build a National Identity Register (NIR). Biographical information will be held on the Department for Work and Pensions (DWP) database; biometric data on the Home Office database, and the remaining details on the Identity and Passport Service (IPS) system.

The shift may be a direct result of criticism towards the lack of security, voiced, among others, by the UK Information Commissioner (ICO) and a group of academics from the London School of Economics (LSE). The ICO pointed out to the government as early as 2003 that there may well be other ways to run an identification system so as to avoid an intrusive central register of personal information. Two years later, the LSE's Identity Project identified several security risks in the government's original thinking, including the plans to build one big database.

Dr Edgar A Whitley, research coordinator for the LSE Identity Project, said at the time of the publication of the new plans:

> The Strategic Action Plan represents a total rethink of the original plans that were proposed by the Home Office. These original plans had been criticized by the LSE Identity Project as being too complex, technically unsafe, overly prescriptive and lacking a foundation of public trust and confidence. Despite their earlier hostility, the government now clearly agrees with us and the LSE team welcomes the marked shift in the government's position that this Action Plan indicates.

Simon Davies, a visiting fellow of the Information Systems group at LSE, and director of Privacy International, was one of the Identity Project's mentors. He observed:

> The original plans involved building a single, secure database for all the identity information that was being recorded. Whilst the new scheme distributes this information around a number of existing databases, what is not clear is whether these existing databases will have the necessary security to ensure that this personal data cannot be compromised. While the government has done the right thing by acknowledging the vast flaws in its original proposals it now faces an almost impossible challenge to build trust. The scheme has become poisoned inside and outside Whitehall.

Publication a low-key event

The ID cards scheme — which is being justified as helping to secure Britain's borders and tackle illegal immigration, reduce fraud, and fight crime and terrorism by providing a secure means of identification — is now in full swing.

The Strategic Action Plan for the National Identity Scheme,[1] which was published just before Christmas last year, follows a wider Home Office review earlier last year, and marks a start for implementing the plans. The ID cards will be introduced to UK citizens in 2009, and biometric residence permits for foreign nationals in 2008.

Commenting on the publication date, Phil Booth, General Secretary of NO2ID's, a campaign group fighting ID cards, said: 'The government clearly tried to 'bury' the action plan. Publishing such a significant document a week late, and just hours before Parliament rose for Christmas, was clearly an attempt to minimise media exposure.'

Three databases

According to the new plans, *biometric details* will be held on the Home Office database that is already used to store biometric details of asylum seekers and those who have applied for biometric visas.

The government plans to use DWP's Customer Information System (CIS) technology to store NIR *biographical information.* According to the Strategic Action Plan:

> DWP's CIS technology is already used to hold records for everyone who has a National Insurance Number — ie nearly everyone in the UK. However, even though the CIS already contains personal details for most adults in the UK, these entries will not simply be copied to the NIR. The details of any individual entered in the NIR will be recorded when they apply and verified to the highest possible standard before being recorded in the NIR.

For British citizens, the National Identity Scheme will be administered by the IPS on behalf of the Home Secretary. The IPS will hold *administrative information* related to the issue and use of ID cards and passports, and will be built on the existing IPS systems. For foreign nationals (including both European economic area (EEA) and non-EEA nationals), authentication, enrolment and the production of documents will ıll be carried out in the early stages by he Immigration and Nationality)irectorate (IND), supported by IPS.

Security concerns vary from ;uaranteeing authorised access to the ystem to storing biometric ıformation. One of the main issues is ·ersonal information that is not part of JIR.

A Home Office spokesman explained that improved security was a major factor behind the change of plan, and even if existing networks are used, all information that will be stored is new.

Phil Booth stressed that as the NIR will be the key to a total life history of every individual, it is of paramount importance that the infrastructure is secure:

> The Home Office is trying to make out that physically separating the data stored on the NIR was partially a security decision but, as any competent technologist would know, even the single 'new, clean database' was always going to have to be distributed across a number of physical devices and/or locations — anything else would have broken fundamental IT security principles.
>
> Spreading the register across three separate networks — each originally designed for a different purpose — will introduce unnecessary complexities and points of vulnerability that could, in effect, make people's personal data far less secure. Even if the Home Office says that they are able to put in place sufficient safeguards and access controls, this is going to be much harder to do across three systems.

Costs will be spread

NO2IDs sees the scrapping of the one big database as a cost-hiding exercise. Booth explained that kludging NIR together by using pre-existing systems will make the build look 'cheaper' is as the costs — and inevitable cost over-runs — will be on the books of other government departments like DWP.

A Home Office spokesman said that spreading costs was never a secret. Eventually, the cards will pay for themselves as applicants will have to pay for their cards, which will initially be manufactured inhouse by the Home Office. According to current plans, cards should be compatible with chip-and-pin technology, and to prevent hacking, the database will not be connected directly to the internet.

No iris scans

Registration to the NIR will eventually, subject to parliamentary approval, be compulsory. The Action Plan says that 'when you enroll into the Scheme, your fingerprint biometrics (all 10 fingerprints) will be recorded and stored in the NIR. A subset of these will be held on your ID card or passport'.

The government has chosen to gather just fingerprints and facial images, and not iris scans. This is apparently because these two biometrics have already been tried and tested. The Home Office insists that the iris-recognition pilot scheme has been a success, and introducing iris scan later on remains an option.

New supervisory body

The government assures that data storage in the NIR will meet the requirements of the UK *Data Protection Act 1998*, but the Information Commissioner has been concerned about the lack of comprehensive powers for the ICO to check on data protection compliance.

Now the government is committed to appointing an independent National Identity Scheme Commissioner to supervise the ID scheme. The Commissioner will not be based in IPS, but will make regular reports to the Home Secretary, which will be laid before Parliament.

The two Commissioners are expected to work close together. While compliance with the *Data Protection Act* will remain under the remit of the Information Commissioner, the National Identity Scheme Commissioner will oversee the uses to which ID cards are put, and the functioning of the scheme. A situation may arise where the two Commissioners will be investigating the same issue — for example, if a complaint is made about leaking address details, the ICO would look at how personal data has been processed, and the National Identity Scheme Commissioner at IPS procedures.

It will be a criminal offence to tamper with the NIR, with a maximum penalty of 10 years' imprisonment for an unauthorised disclosure of information.

Conclusion

While the government says that the early needs of creating NIR will be met by using the existing biometric storage and matching systems from within IPS and the Immigration and Nationality Directorate (IND), in the future private sector assistance will be needed. A procurement process on creating additional security measures is planned to begin formally in the second quarter of 2007.

Judging from a cautious approach in building NIR, the government seems to be mindful of recent IT network disasters and does not want to introduce too much change at one point. However, the foreword of the Action Plan says that the ID scheme 'will evolve over time', and that 'we shall adjust the details of this action plan as required by experience' — in other words, anything is possible. ●

Laura Linkomies.

This article was first published in the Privacy Laws & Business UK Newsletter, *Issue 30 (February 2007); <www.privacylaws.com>.*

Endnote

1. See <www.identitycards.gov.uk/downloads/Strategic_Action_Plan.pdf>.