Australian Privacy Foundation

Document verification and identity management

Presentation by Anna Johnston, Chair, Australian Privacy Foundation

Safeguarding Australia 2005
The 4th Homeland Security Summit & Exposition
12 July 2005, Canberra

Good afternoon.

I would like to thank the conference organisers for their invitation to address this summit.

The Australian Privacy Foundation was formed in 1987, and is the leading non-governmental organisation dedicated to protecting the privacy rights of Australians. We aim to focus public attention on emerging issues which pose a threat to the freedom and privacy of Australians. For further information I invite you to take a look at our website at www.privacy.org.au.

At the outset I wish to state that we appreciate privacy is not an absolute interest. Privacy must be balanced against other public interests such as law enforcement and national security – but we will be concerned to know that the balance is right.

Our concern will usually be raised whenever a new policy is proposed that would introduce some element of surveillance or 'dataveillance' of the whole population, not just those who are genuine suspects.

This is the basis of our interest in many of the strategies, laws and policies developed to combat terrorism.

The danger of laws and practices which erode our privacy, whether they be street surveillance or the sharing of personal information between government agencies, is that they treat the average person as a suspect rather than a citizen. In such circumstances the government treats us all 'as if we are hiding something'[1].

As then Professor Zelman Cowen said in the 1969 Boyer lectures, "A man without privacy is a man without dignity; the fear that Big Brother is watching and listening threatens the freedom of the individual no less than the prison bars"[2].

Now turning to terrorism as the theme of this conference. We have previously expressed our concern at the extent to which the 'war on terror' is used to justify an abandonment of rationality in our policy processes, such that new proposals are not calmly weighed in terms of necessity, proportionality or 'reasonableness', effectiveness, and alternative options.

It is important to stress that the identity management systems and strategies discussed here today will not present any kind of magic prevention or cure for the evils of terrorism. In particular, it should not go unsaid that in its lengthy deliberations on the September 11 attacks in America, the 9/11 Commission did *not* recommend the introduction of national ID cards, or anything of the sort.

There is often this kind of intuitive response to terrorism, or other crimes, along the lines of – "well if we just knew who everybody was, and what they were doing, then we'd be able to pick out the bad apples". We disagree, especially if more targeted efforts can yield better results.

For example a recent US Government Accountability Office report into passport fraud found a number of factors were inhibiting the State Department's ability to prevent or detect the issuing of fraudulent passports to known or suspected criminals and terrorists[3]. (They found 37 out of 67 names of known fugitives they tested, including one from the FBI's "Ten Most Wanted" list, were not on the State Department's watch-list. These were people suspected of crimes including murder, bombings and child sex offences.)

The factors found to be inhibiting the prevention of passport fraud included staffing reductions, workload levels, insufficient training and insufficient oversight.

I'm not suggesting that Australian agencies are equally ill-equipped – I wouldn't know. I am merely using this as an example of where existing processes and laws should be utilised in a targeted way against people genuinely suspected of crimes, including terrorism, instead of thinking that we should instead introduce sweeping powers to scoop up everyone in wider and wider nets of mass surveillance and data-matching programs, in the hope of finding the needle in the haystack.

And dealing with any staffing and resourcing issues wouldn't be a bad place to start.

[1] Dr Caoifhionn Gallagher, "Nothing to hide, nothing to fear? Privacy v. Government", in *Liberty*, Autumn 2003.

[2] Zelman Cowen, 1969, 'The Private Man', *The Boyer Lectures*, Australian Broadcasting Commission, pp 9-10.

[3] United States Government Accountability Office, *State Department: Improvements Needed to Strengthen U.S. Passport Fraud Detection Efforts*, Report # GAO-05-477, 20 May 2005, available at www.gao.gov

So we are going to be opposed to any proposal that looks or smells like a national identity card, especially if it is being touted as the cure for terrorism.

In this respect we are extremely pleased that the Australian Government has repeatedly assured us that not only does it have no intention to introduce such a proposal, but that Senator Ellison and the Attorney General Philip Ruddock[4] have both also demonstrated their understanding that a system which relies on a single identity document is ultimately doomed to make the problems of identity fraud and identity theft so much worse.

There are a number of reasons for this. First, as we have heard from other speakers today, a central database model makes it easier for the organised criminal or terrorist to steal a real identity or create a new fake one - they only have to bribe one person, or hack into one system, or forge one document, or fool one agency, instead of many.

Second, the greater the perceived value of a particular document in proving identity, the greater is its value to organised criminals. Individuals, businesses and government agencies will come to rely on this one document as a single ‘proof of identity’. This false sense of security allows reliance on a piece of plastic as evidence of a person’s honest intentions, instead of exercising common sense or precaution. That is, by creating a single trusted identity document, the government would also be creating a new opportunity for organised criminals and terrorists to fool a complacent public.

A single centralised identity model also makes the repercussions of identity theft worse for the victim, as the degree of privacy invasion is greater, and the ability for a person to remedy a theft of their identity is more complex[5].

So centralising identity management increases both the risk of identity theft, and the degree of harm suffered by the victim when it occurs. For these reasons the Australian Government and the United States Government have recognised the security flaws in creating or relying on a single identity document or single database[6].

That brings us to the Australian Government’s national identity security strategy, and the various projects being piloted.

The Document Verification System is about rooting out the problem of fake foundation documents, such as the fake driver’s licence or birth certificate being used to apply for a passport or for social security benefits.

From what we understand to date about the Document Verification System being proposed, its strength is firstly in its support for a dispersed identity model, and secondly

[4] Attorney General Philip Ruddock said in a speech on 29 June 2005: “We do not support the approach where all personal information is centralised on one database, and a single form of identification is issued. This could increase the risk of fraud because only one document would need to be counterfeited to establish identity”. Senator Chris Ellison said before budget estimates on 23 May 2005: “I do not mean an Australia Card – we have ruled that out – but a much more secure system where you can rely on two or three documents and have them crosschecked across jurisdictions ...”

[5] The inclusion of biometric data can make this process even more difficult for the innocent victim of identity theft; once a biometric other than theirs is associated with their data in a trusted database (whether through error or fraud), it is extremely difficult for the person to prove otherwise.

[6] See a discussion of the recommendations of the US Federal Advisory Committee on False Identification in *Your Papers Please: From the State drivers license to a national identification system*, Electronic Privacy Information Center, February 2002, available at www.epic.org

because it is intended to work in a way to minimise privacy intrusions. The system itself is supposed to be 'blind' and to hold no data; the agency being asked to verify its document does not know the identity of the organisation asking the question; and the questioning agency is only given a minimal yes/no response.

But it is important to also recognise that the DVS cannot alone solve all identity fraud and theft.

Firstly of course, there are many different kinds of identity-based fraud. We would like to know more about what kinds of identity fraud are likely to be detected by DVS? Are we talking about 17 year olds getting fake licences just so they can go to the pub, are we talking about so-called 'welfare cheats'[7], or are we talking about organised criminals or terrorists using ID as a tool to commit greater crimes?

I suspect the latter will just get more organised and work through the other points of weakness, for example by using bribery or hacking at the document-issuing agency to create 'real' IDs, but with fake details on them. (For example seven of the hijackers in the September 11 attacks in America had *genuine* driver's licences, which they obtained for between US$50 and $100[8].)

So we would like to see a lot more detail on the national identity security strategy. Some of the questions which should be asked of the various projects like DVS are:

- what is the cost of the problem? (best estimate to date is A$1 billion pa)
- what will be the cost of the strategy to address the problem? (is the response proportional?)
- what impact will the strategy have on the problem? (will it make a positive net impact on identity fraud and theft?)
- what consideration has been given to alternative designs or ways of addressing the problem, in order to lower the cost and/or minimise privacy and other risks?
- and what might undermine the effectiveness of the strategy?

I would like to just briefly provide a few pointers, rather than answers, to these questions.

The first is with respect to costs – I'd like to quote you a few figures from the UK, where they are right now considering a bill to introduce national identity cards.

In the UK, the cost of identity fraud is estimated at up to £1.3 billion pa.

It has been estimated that only £35 million pa of this – or less than a third - could be eliminated with a national identity card.

The direct costs to government alone (i.e. not including businesses who must buy readers to use the cards) over the 10-yr period proposed for introducing the UK national

[7] University of Queensland research into 75 welfare fraud cases found that the cases involved sums of $5,000 to $10,000, and none involved the use of multiple identities; see Adele Horin, "Cheats turn out to be on the margins", *Sydney Morning Herald*, 9 July 2005.

[8] See Matthew Barakat, "Hijackers' bogus identification cards prompt scrutiny of state licensing rules", *San Francisco Chronicle*, 9 October 2001, available at www.sfgate.com.

identity card, has been estimated by the London School of Economics at between £10.6 billion and £19.2 billion, with a median figure of £14.5 billion[9].

When you break that down to a yearly figure, the cost of the solution is likely to be at least four times higher than the cost of problem that will be fixed.

You can see why the economists are scratching their heads over the proposal, even leaving aside the various objections along privacy grounds.

And what might undermine the effectiveness of the strategy?

In relation to federal, State and Territory government involvement in the national identity security strategy, Senator Ellison has said[10]: “You either do it all together or you do not do it at all”.

But does the left hand know what the right hand is doing? Are you all singing from the same song-sheet in terms of the importance of maintaining dispersed identity management systems rather than centralised systems?

I would ask the Senator:

- what are your fellow Ministers doing?

Joe Hockey has started going on about a Medicare smartcard to be used for accessing other government services. And Tony Abbott recently said he saw nothing wrong with the idea of putting everyone’s health information into one big national database.

- and what are the States doing?

The Queensland government has been looking at a smartcard driver’s licence that could be used for other applications as well.

And NSW just passed a new Act to allow the Roads and Traffic Authority to issue photo identity cards to non-drivers – with their information held on the same database as for drivers, and the cards to be issued will be effectively the same as a driver’s licence. The card number – whether it is a driver’s licence or the non-driver card – will therefore feature a unique and near universal identification number. So all of a sudden in NSW we’ll effectively have a single identity card, with all the weaknesses that means for actually tackling the problems of identity fraud and theft.

It would seem to us that unfortunately not everyone is yet on board the national identity security strategy. The message about how to tackle identity fraud is not getting through – and as a result we risk making the problem worse

In conclusion I would suggest that the Australian government must do the same kind of comprehensive cost / benefit analysis we’ve seen in the UK – including demonstrating which type of identity fraud will be fixed, and to what degree.

[9] The LSE Identity Project Report, June 2005.
[10] Senator Ellison, budget estimates on 23 May 2005.

Then we can conduct some better informed policy debates around these proposals – to see what Australians think about the costs and benefits, whether the proposals are a proportionate and fair response to the risk, whether they are necessary, whether they will be effective, and whether there are better alternatives.

But if the right hand doesn't know what the left hand is doing, or if we don't have those more transparent public debates, we may be sleepwalking into a database state - in which we will have lost our privacy, and gained no additional security, because we will have made the identity management problems worse instead of better.