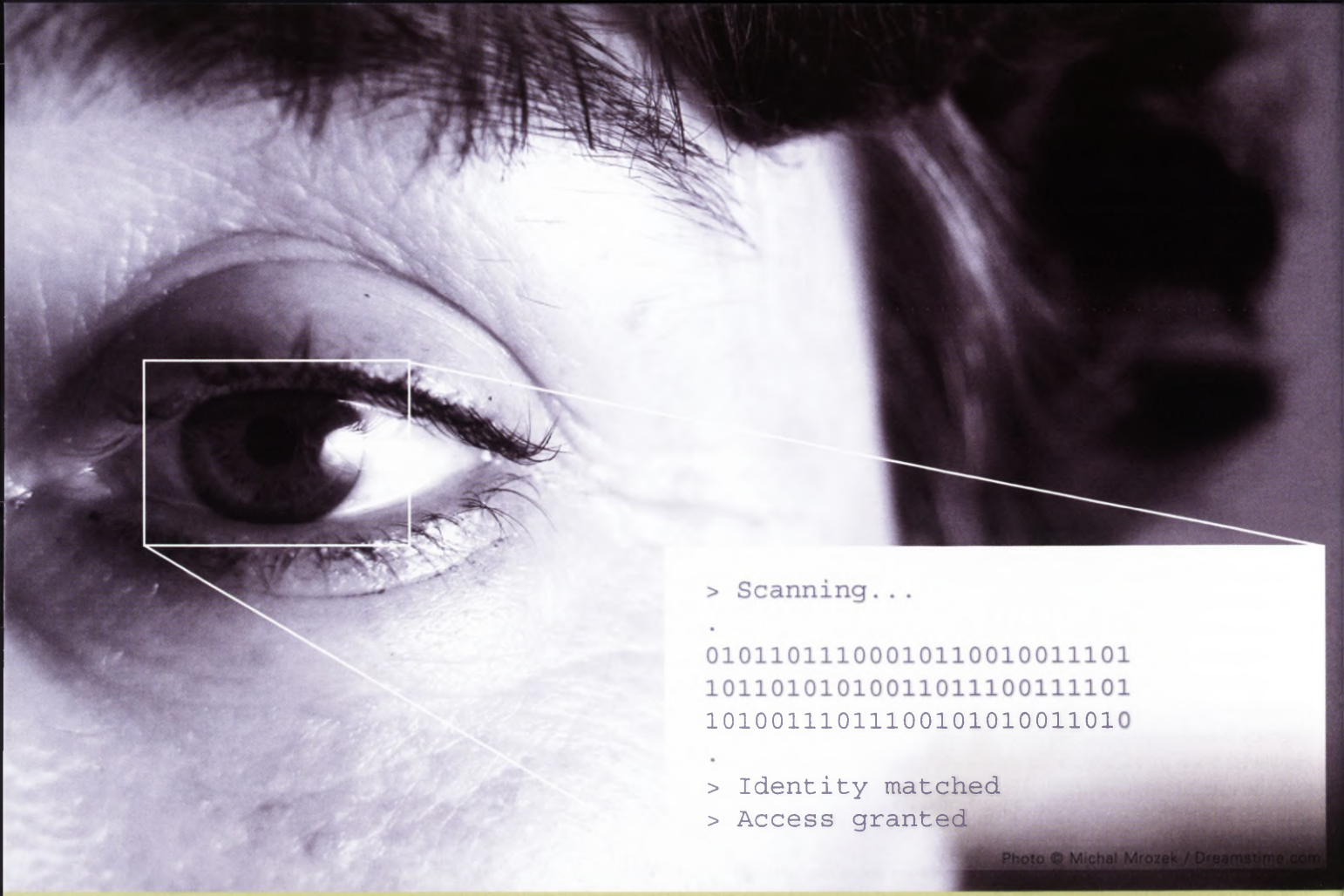

The proposed 'access card'

why we need a national id card debate

By Graham Greenleaf

Trusting politicians to protect privacy is risky.

Twenty years ago, the Hawke-Keating government announced a national identification (ID) system with the patriotically named 'Australia Card' as its centrepiece. It received much public support and was the ostensible cause of a successful double-dissolution election that resulted in a Labor victory. But 18 months later, it was so despised by most Australians that it was withdrawn after a fatal drafting flaw was found in its enabling legislation. Its successor, the tax file number system, removed the card and the central computer register, and added more serious privacy protections. Although it represented a reasonable political compromise at the time, Keating had reneged on promises not to expand it within two years, and 'data-matching' had linked it to the social welfare system.

Two decades later, the Howard government vehemently denies that its proposed 'health and social services access card' (the Access Card) is a national ID card, saying that it rejected such an option. To decide whether this claim is true, comparison with the Australia Card proposal is worthwhile.

The Access Card will effectively be compulsory and near-universal for adults, as was the Australia Card. Like the Australia Card, it will not have to be carried at all times, but will only need to be produced for certain transactions.

The Australia Card was primitive compared with its 21st century successor, a 'smart card' that will have considerable chip storage capacity. The data on the face of the Access Card resembles the Australia Card: a unique, universal, compulsory national ID number; name; photograph; signature and card expiry date. The Access Card will also record an up-to-date address, date of birth, details of children and other dependants. The chip will also hold extensive optional data including medical information, and an 'electronic purse' for which the only use as yet announced is to make emergency welfare payments directly to the card. In addition to its likely capacity to store much more information than this, every aspect of the stored content of the Access Card, its accessibility and security, presents far greater dangers than did the Australia Card.

As with all ID systems, the card is only the visible part. The back-end computer systems are just as important. Both the Australia Card and the Access Card systems depend on a central register: the Australia Card Register and now the 'Secure Customer Registration System' (SCRS). While the first contained little more than identification information and a current address, the SCRS will also contain a copy of all the emergency contact, medical and other information 'to allow lost cards to be replaced';[1] concession status; and a copy of all documents initially produced by a person to establish their identity, such as birth certificates. It would be hard to imagine a better source for ID fraud, but the government's consultants claim it 'will not contain any sensitive personal information'.[2]

SCRS will be the only comprehensive photographic database of Australians and will allow 'one-to-many matching':[3] a national, searchable, photo library technically capable of searching for photos of people appearing in CCTV tapes, or in photos taken at demonstrations and strikes. Fortunately no such uses have yet been proposed. The proposed extent of networked access to the two registers is much the same as far as government agencies are concerned but, this time, whenever a person visits a GP or pharmacist, their card will be used to check their eligibility for non-permanent concessions with SCRS.

The Australia Card came with a legislative package that included measures – albeit flawed – to limit potential uses of the number and the card. But the government's current proposals on this point are still extremely vague.

This time around, the government has a docile rather than a hostile senate, so we can expect no deliverance from that direction. What we need is a national debate about whether we want a national ID card – otherwise we will have such a card imposed on us.

THE TASKFORCE REPORT – A SHEEP IN WOLF'S CLOTHING

Professor Alan Fels, former competition regulator, heads the 'Consumer and Privacy Taskforce', which is charged with advising the Minister for Human Services, Joe Hockey, on the proposed Access Card. The taskforce also includes a former NSW privacy commissioner (Chris Puplick) and a former deputy defence ombudsman (John Wood). The taskforce has no statutory basis or detailed terms of reference, and must report to the minister (not the public). It is nonetheless perceived by the media, politicians and public to be an independent watchdog over this proposal, because of the presumed credibility of its members. It published its first report, containing 26 recommendations, on 8 November 2006, to which the government has already responded.

Is the taskforce living up to expectations, on the evidence of this report and its recommendations? If a national debate is required, as suggested above, is it helping to create one?

The report sheds no new light on the as-yet sketchy details of the government's proposals, which were not available at the time of its background paper almost nine months ago. Whatever the taskforce has learned, the government doesn't want it to say. To the suggestion that information concerning chip capacity (R22) should be made publicly available, the government has somewhat evasively responded that it (not the taskforce) can easily publish such information 'when it becomes available'. In other words, the less the public is >>

told the better. Nor has the government released the Privacy Impact Assessment on the proposal that it received over nine months ago. Its repeated protestations of intended transparency therefore continue to ring hollow.

Does the taskforce make any substantive recommendations? First is a category that could politely be called 'uncontroversial':

- Human Services Minister Hockey, in a speech to the National Press Club, successfully focused media attention on government acceptance of the taskforce recommendation that individuals should have 'ownership' of their Access Card (R8). This is different from the ownership of passports, credit cards, etc, which remain the property of the issuing party. Touted as some kind of privacy protection and a guarantee that the Access Card will not become an ID card, this is an exceptionally silly and trivial proposal. Ownership of a physical token provides nothing except some protection against confiscation (which becomes larceny). What is important about ID cards is that others wish to see them (for the photo, name and signature), copy details (the ID number) or scan them (the chip content), none of which has any particularly relevance to property in the physical token. If anything, this is a *reductio ad absurdum* of property as privacy protection.
- The face of a card should be able to show your alias, provided its use is not deceptive (R10). It would be surprising and alarming if people in the entertainment industry or others who legitimately use names other than their given name in daily life could not do so, so this was accepted. However, an unexpected sting was revealed in the minister's speech: if you use an alias, the chip on your card will also contain your 'real' name. So from now on, anyone who suspects that a person uses an alias will know exactly where their 'real' name can be found. This is not a win for privacy, but a potential disaster for anyone with an alias.
- The taskforce's recommendation that the expiry date should be on the card (R19) was also accepted.

So much for the weighty recommendations that the government accepted. What about those it rejected?

- The taskforce saw 'great merit' in people's photos being stored only in the back-end database as a template and not as actual photos (R12). This significant recommendation was rejected by the government. But because it was combined with an uncontroversial recommendation for 'rigorous controls', which was accepted, the government claimed to have accepted the whole package.
- The taskforce recommended that no signature be visible on the card (R15), but the government rejected this because a signature will 'make it easier to cross-check signatures'[4] on paper forms.
- The taskforce suggested that the ID number should not be visible on the card (R18), but the government rejected this to 'make it quicker and easier for people to use the card for telephone and online services'.[5]
- The taskforce made the very important recommendation that proof of identity (POI) documents, produced when a person registers for a card, should not be scanned, copied or permanently stored online in the back-end database once they have been verified (R20), contrary to the extraordinarily intrusive recommendation of the KPMG 'business case'. The government's response is that it 'partially supports' this recommendation, adding that it 'will explore relevant legislation and business procedures with a view to implementing this recommendation'.[6] In other words 'we will tell you later which data we would like to keep forever, but we might not keep everything'.

Ultimately, then, every single taskforce recommendation that would seriously restrict the surveillance potential of the ID card system has either been rejected by the government or obfuscated sufficiently to allow future rejection.

Two other taskforce recommendations in key areas (the national photo database in R12 and the national signature database in R16) boil down to little more than a warning of serious risks, and the consequent need for strong security controls. One would have to be foolish to disagree with that. But no particular security requirements are specified, or anything of substance suggested by way of appropriate criminal offences or damages for misuse or abuse of information stored on the card. Hong Kong's recent experience, where 20,000 police complaint files from the previously presumed high-security Independent Police Complaints Council appeared on the internet, gives an indication of the stakes involved.[7] >>

Despite the taskforce's detailed and significant criticisms of the government's plans, and specific suggestions of things that could or should be done, its actual recommendations are almost always much weaker than the arguments that it has presented and apparently endorsed. In most cases, the recommendations merely request further information or additional consultation, giving the government scope to formally agree with them without endorsing any substantial or meaningful changes. Eleven of the 26 recommendations can be summarised as 'provide more information' (R1, 2, 3, 4, 5, 13, 14, 15, 17, 23, 26). Another three boil down to 'consult further' (R21, 24, 25).

That leaves one last case of anaemia. The taskforce recommends 'a comprehensive legislative framework for the Access Card scheme' (R6), but doesn't say what it should include, only that its views on the legislation should be taken into account as it develops (R7). The taskforce declines to recommend anything specific, saying that it 'is not in a position to provide a definitive statement or list about what matters should be comprehended in legislation',[8] even though it gives a long list of such matters in its argument. This gives the government the opportunity to agree without assenting to anything much beyond the fact that there will be legislation governing the Access Card. For example, the taskforce says (but does not recommend) that legislation should 'clearly address at least three broad issues' including preventing 'function creep' (or 'transparency mechanisms' for adding new uses), and control of the back-end database. But when the government lists what the legislation will contain, it is able to ignore both of these key issues while ostensibly accepting the recommendation.

Thus the taskforce report is ultimately falsely reassuring, all pretence of fierce protection of the public but without any bite. Its vague recommendations allow the government to convince the press that it is 'accepting almost all of Professor Fels' recommendations',[9] giving the impression that government and taskforce are united and marching toward the future now that privacy protection is secure.

The taskforce avoids making any recommendations about many crucial aspects of the ID scheme's infrastructure. What limitations should apply to its use by both the private and public sectors? All the report says is that it will be legally difficult to control what state governments do. How can the private sector be prevented from circumventing prohibitions on its demanding to see the card simply by making it too inconvenient for people to produce anything else that is satisfactory? This is just one example of the serious issues that have been left untackled.

The taskforce states that:

> 'Since the idea of having a national identity card has been clearly ruled out by the government and according to public opinion polls is not supported by the Australian public either, it becomes important to ensure that the health and social services Access Card does not become, now or in the future, a national identity card by any other name.'[10]

Statements like these would have borne much more weight had the taskforce used its recommendations to set out in detail what can be done to ensure that the Access Card does not become a national ID system, rather than avoiding this crucial issue. ■

Notes: **1** KPMG Health and Social Services Smart Card Initiative, *Vol. 1: Business Case* (Public Extract), released 6 June 2006. **2** *Ibid.* **3** *Ibid.* **4** Australian government's response to the *Access Card Consumer and Privacy Taskforce's Advice to the Minister for Human Services*, November 2006. **5** *Ibid.* **6** *Ibid.* **7** See Greenleaf, *Privacy Laws & Business International*, Issue 84, p13 and Issue 82, p10. **8** Access Card Consumer and Privacy Taskforce, *Issues and Recommendations in Relation to Architecture Questions of the Access Card*, 25 September 2006. **9** ABC Radio National Breakfast, 9 November 2006, transcript of interview of Prof Alan Fels by Fran Kelly. **10** *Ibid.*

Graham Greenleaf *is co-director of the Cyberspace Law & Policy Centre, Faculty of Law, UNSW, and a member of the Board of the Australian Privacy Foundation and Asian-Pacific editor of Privacy Laws and Business.* **PHONE** *(02) 9385 2233*
EMAIL *graham@austlii.edu.au*

Earlier versions of parts of this article were published in the UNSW magazine, *Uniken*, and in *Privacy Laws & Business International*, a UK journal. It was written before the December 2006 technical briefings on the Access Card and does not take it, or the draft legislation subsequently released in December, into account.