



**Australian
Privacy
Foundation**

post: GPO Box 1196
Sydney NSW 2001
email: mail@privacy.org.au
web: www.privacy.org.au

AusCheck Bill 2006

Submission to

Senate Legal & Constitutional Committee

February 2007

The Australian Privacy Foundation

The Australian Privacy Foundation (APF) 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.

Since 1987 the Australian Privacy Foundation has led the defence of the rights of individuals to control their personal information and to be free of excessive intrusions. We use the Australian Privacy Charter as a benchmark against which laws, regulations and privacy invasive initiatives can be assessed.

For further information about the Foundation, see www.privacy.org.au

Introduction

This Bill authorises the establishment of a very significant new identity management system, which is expressly designed to go well beyond its initial application to Aviation and Maritime Security identification cards.¹

We understand that a Privacy Impact Assessment (PIA) on the AusCheck scheme is in progress (we were invited to provide input and have submitted an early draft of this submission. The timing is not sensible – any PIA should be made public to assist interested parties to assess the Bill. PIAs should not be used a confidential resource by agencies to anticipate and head off criticism – their public interest value lies in the contribution they make to informed public debate. We submit that the Committee should recommend that the government publish any PIA report on the scheme as soon as possible, but certainly before any further parliamentary debate.

General Comments

Our analysis of the Bill was not assisted by fact that the Explanatory Memorandum refers to non-existent clauses (e.g. clause 45 and clause 25). This is not helpful to any interested party and we request that the Committee point this out to the Department.

There have been media reports of significant weaknesses and failures in the existing system for managing Aviation and Maritime Security identification cards. While the proposed legislation may go some way to improving the integrity and security of the system, the failures to date should underline the inherent difficulty of managing identities, and force a recognition that the ‘holy grail’ of a foolproof system is realistically unachievable.

Any centralised database of individuals’ identity information and supporting documentation is also a potential ‘honeypot’ for criminals intent on identity theft or fraud. It is an unavoidable paradox that any ID

¹ Clause 8(2) makes it clear that the scheme could apply to checks for any purposes within the constitutional competence of the Commonwealth.

system designed to improve security also increases the risk, and potentially damaging consequences, of any security breach.

In recognition of these two facts it is essential that there should be a balanced 'risk management' approach to the privacy intrusion inherent in any identity management system. Instead of pursuing an ultimately unachievable objective of perfection, with more and more privacy intrusive elements, the Commonwealth government should accept a more decentralised 'purpose-specific' approach, in which individuals are only required to surrender personal information, and submit to checks, that are proportional to the risk in the particular context in which they need to be identified.

The EM explains that the Bill 'establishes a regulatory framework within which a government agency can provide centralised background checking coordination to a wide range of government agencies'. It is also implicit that AusCheck will provide these services from the outset to the private sector aviation and maritime industries, and the Bill expressly allows for the scheme to be used in other private sector contexts.

A major risk in this new centralised multi-purpose identification and checking scheme is that it adopts a 'highest common requirement' meaning that individuals' privacy is intruded on unnecessarily in contexts where a lower standard would suffice.

We submit that a fundamental design element of the AusCheck scheme must be a layered approach, rather than a single 'one-size-fits-all' approach.

Specific Comments

This section identifies and briefly comments on the most serious problems which APF has identified concerning the aspects of the AusCheck scheme that are disclosed in this Bill.

Too much of the detail about the scheme design and operation is left to Regulations. We submit that this leaves too much discretion to the Minister and Department, and that more of the basic parameters of the Scheme need to be specified in the primary legislation.

We understand from the Second reading speech that the checking process will make use of the Commonwealth Document Verification Service (DVS). Despite the announcement of this Service some years ago, very few details have been made public, although answers to Senate Estimates Committee questions in February 2007 on the Access Card suggest the DVS may not be fully functional until 2010. It is impossible to fully assess the privacy implications of this Bill without more information about the DVS. We submit that the Committee should recommend that the government publish detailed information about the design of the DVS and progress in establishing it and the rules on who will have access to it for what purposes.

The definition of 'background check' in clause 5 only specifies criminal history and citizenship or residency status, but also includes (b) any 'matters relevant to a security assessment' and (d) other matters to be specified by Regulation. No further guidance is given as to what other matters might be relevant, apparently leaving it entirely to the discretion of the scheme administrators as what other information can be collected. Neither are there any criteria for what additional details might be required by Regulations. It is not clear why this power is necessary if anything relevant can already be collected under (b) – it is surely not envisaged that Regulations might allow for the collection of irrelevant information?

Specifically, there is no indication even of what 'criminal history' will be collected and held, and Federal, State and Territory spent convictions schemes do not seem to be taken into account. We reject any assumption that any and all encounters with the criminal justice system are necessarily relevant to an individual's suitability for the open-ended range of 'positions' or 'activities' for which the AusCheck system will be used. In this respect we draw the Committee's attention to the June 2006 report by the Victorian Privacy Commissioner to the Victorian Attorney-General on Controlled Disclosure of Criminal Record Information.

Overall, clause 5 means that there are no limits on what personal information might be required. This is completely unacceptable.

Clause 10 provides for the AusCheck scheme to require individuals to submit to background checks in a potentially unlimited range of contexts. We submit that it is not appropriate to locate the requirement for a check in legislation which should be about the establishment and operation of the checking 'infrastructure'. The requirements for a check should be in other specific legislation dealing with particular jobs or roles, such as some of those in the maritime and aviation industries. It is appropriate for the AusCheck scheme to keep a central register of the purposes for which checks are required, but it should not itself be the source of the authority for checks.

Clause 14(2)(b)(iii) provides that any information included in the AusCheck database will be able to be used for 'criminal intelligence and security intelligence'. These two terms are undefined and the result is a much broader exception than the 'law enforcement' exceptions to IPPs 10 & 11 of the Privacy Act, which implement the fundamental privacy principle that information should only be used or disclosed for the purpose for which it is collected. It is not clear why AusCheck cannot operate as intended without additional authority for use and disclosure.

It is completely unacceptable for the AusCheck database to be available as a general intelligence resource for an unspecified range of agencies for such undefined purposes.

Clause 14 also authorises the retention of personal information in the AusCheck database, but without any specified retention criteria or periods. This allows the information to be kept indefinitely. While there are no express retention or disposal rules in the now outdated Information Privacy Principles applying to Commonwealth agencies under the Privacy Act², the absence of any limits is inconsistent with the spirit of privacy laws (as expressed for the private sector in national Privacy Principle 4(2) and for State government agencies in the equivalent principles in the NSW, Victorian and NT privacy laws. We submit that the Bill should specify retention periods or at least criteria for disposal – there is no reason why personal information about someone who is no longer subject to any security check requirement needs to be retained indefinitely.

Conclusions

This Bill is fundamentally flawed in that it authorises the establishment of a background checking infrastructure with very few limits on what information can be held in the database; the purposes for which it can be used or the range of bodies to be covered by the scheme and given access to the database. It is a wholly disproportionate general response to a series of specific needs, and offends against a number of information privacy principles.

² The absence of a retention/disposal principle has been identified as a key issue by the current ALRC Review of the Privacy Act – Issues Paper paragraphs 4.116 & 4.120-122 and Q.4-18)
<http://www.austlii.edu.au/au/other/alrc/publications/issues/31/>