Australian Privacy Foundation

post: GPO Box 1196
Sydney NSW 2001

email: enquiries@privacy.org.au

web: www.privacy.org.au

1 March 2006

Senate Finance and Public Administration Committee
VIA EMAIL: fpa.sen@aph.gov.au

Inquiry into the Electoral and Referendum Amendment (Electoral Integrity and Other Measures) Bill 2005

Re: Electoral and Referendum Amendment (Electoral Integrity and Other Measures) Bill 2005

Dear Senators,

We regret that we only became aware that this Bill had been referred to the Committee a few days ago, and have not had time to comprehensively analyse the Bill in relation to its privacy implications.

We do however have particular concerns about the evidence of identity provisions for electoral enrolment, and about the extension of the Australian Electoral Commission (AEC)'s demand for information powers.

Evidence of Identity

We understand that these proposed provisions supersede amendments already enacted in 2004, but which have not yet been implemented. The new requirements are even more stringent, requiring an enrolment application to be accompanied by either:

- a drivers licence number for the applicant, or
- attestation by one of a prescribed class of electors who has sighted another prescribed form evidence of the applicant's identity, or
- declarations by two referees that they have known the applicant for at least a month.

These are minimum statutory requirements – the implementing Regulations may impose additional requirements.

Similar evidence of identity requirements will apply to provisional voting.

We submit that the evidence of identity requirements on enrolment have more to do with a wider identity management agenda than with the integrity of the electoral roll. We understand that Federal and State Electoral Commissioners have consistently maintained that there is no empirical evidence of significant fraudulent enrolment or fraudulent voting as a result of current enrolment processes, and this was referred to by the minority in the JSCEM report on the 2004 federal election.

It is significant that recent amendments to the Electoral and Referendum Regulations provided for access to the electoral roll by organisations with customer identification obligations under the Financial Transaction Reports Act 1988. While implementation of this access has been delayed, it confirms a trend towards increasing use of the Commonwealth Electoral Roll as a general resource for identity verification and data-matching purposes. This is in marked contrast to the developments at the State level, particularly in Victoria, where the new Electoral Act in 2002 significantly tightened access for purposes other than those directly connected with the operation of the electoral system.

We submit that the need for enhanced evidence of identity requirements, both for enrolment and for provisional voting, has not been demonstrated and that these provisions of the Bill should not be enacted without better justification, and more restrictions on the use of electoral enrolment information for non electoral purposes.

AEC's demand for information powers

The Bill provides for expansion of the AEC's demand power in section 92(1) of the Electoral Act, to enable access to information held by State and Territory Government agencies for the purpose of preparing, maintaining and revising the rolls. The AEC will be able to demand information from any State or Territory agency rather than, as now, only certain specified agencies.

We submit that this again has more to do with enhancing the value of the electoral roll as a general identity management resource than it does with integrity of the roll. It also denies the sovereignty of the States and Territories to set the parameters under which personal information held by them for other purposes should be disclosed.

The amendments to s.92(1) should not be enacted, without a fuller review and debate about the ever-increasing uses of the electoral roll for non-electoral purposes, contrary to established privacy principles.

Risk to data integrity and basic privacy protections

Our system of compulsory voting forces people to reveal personal information about themselves to all levels of government - information which is easy to abuse for other purposes. Any non electoral use of electoral roll data compromises the core principle of privacy protection, that use of personal information should be limited to only pursuing the core purpose for which it was collected.

If Australians become concerned at the use of their electoral roll information for non electoral purposes, there is a risk that some will take action to protect their privacy by subverting the system.

For example, whether warranted or not, fear of being tracked down by debt collectors, the Tax Office or because of an unpaid parking fine provides a greater

incentive for people to provide inaccurate address details to the AEC, or to simply fail to update their address when they move.

At such a point the integrity of AEC electoral roll data will start to diminish, rather than being strengthened.

Given the current absence of demonstrated electoral fraud as noted above, the result could cause a weakening in the integrity of the electoral system, and thus prove a counter-productive exercise.

Yours sincerely

Anna Johnston
Chair, Australian Privacy Foundation

Phone: (02) 9432 0320
E-mail: enquiries@privacy.org.au
Web site: http://www.privacy.org.au

About the Australian Privacy Foundation

The Australian Privacy Foundation 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 us see www.privacy.org.au