Australian Privacy Foundation

p o s t: GPO Box 1196
Sydney NSW 2001

e m a i l: chair@privacy.org.au

w e b : www.privacy.org.au

16 January 2006

Committee Secretary
Senate Legal and Constitutional Committee
Department of the Senate
Parliament House
Canberra ACT 2600

Re: Australian Citizenship Bill 2005 – adoption and disclosure of biometric identifiers

Dear Senators,

I regret that the Australian Privacy Foundation has not had time to respond to this Bill in detail - as an all-volunteer association we are currently overwhelmed by the volume of privacy intrusive measures currently being proposed by various levels of Government, and deserving of comment.

However we would like to offer the following brief comments, regarding the introduction of new biometric identifiers in the citizenship process, and the excessive uses to which such information may be put under this Bill.

In particular, we wish to draw to your attention the fact that the so-called limitations on disclosing personal information, including biometric identifiers, create no real limitations at all.

The adoption of new biometrics

The Australian Privacy Foundation is concerned at the proposal to collect, use and disclose biometric identifiers about applicants for citizenship (and indeed Australian citizens simply seeking proof of their existing status), in the absence of either justification or proof of the efficacy of such technologies, or indeed any widespread public consultation about these developments.

Biometrics and the recording of biometrics in a database form are not infallible technologies. Furthermore databases holding biometric information can be corrupted or subject to human error, as can the public servants with access to the databases. Yet unlike other forms of identifiers or information about a person, if the data is corrupted, the body parts which supply the biometric cannot be replaced. The repercussions for a victim of identity fraud or theft, where biometrics are involved instead of other types of personal information, are much more serious.

This risk presents one reason why the Australian Government ought not be rushing to embrace biometric technology without more careful consideration.

A further reason is that the Australian Government has not yet shown it can manage existing data sets in a way that minimises data error; indeed the Auditor General has pointed to a startling 30% error rate in DIMIA's databases. The Palmer report furthermore identified problems with training of DIMIA staff or understanding of their responsibilities.

To add new forms of data into the mix, without first fixing the underlying problems, and to deploy the collection, storage and matching of biometrics on a vast scale, will likely only compound the problems of misidentification of individuals, leading to results ranging from minor delays or inconvenience to devastating travesties of justice such as wrongful detention or detention of Australians.

A third reason to reject the introduction of biometrics in relation to applications for citizenship is that this can be seen as the 'stalking horse' for a biometric-based national identity card. In today's *Australian Financial Review* for example, the Attorney General Philip Ruddock has suggested a national identity card is all but a *fait accompli*, because some passports already have a biometric (photograph).

The potential unfettered uses of the new biometrics

Clauses 42 and 43 of the Bill purport to set limits on the use and disclosure of personal identifiers collected for citizenship purposes. In fact almost no limitations are placed on disclosures at all.

Our reading of those clauses is that identifying information about citizenship applicants, including fingerprints, photographs and iris scans, could be accessed or disclosed for any reason, so long as there is either:

- a law allowing the recipient to access such information (cl.42(4)(h)), or
- a purpose of data-matching to identify a person for citizenship purposes (cl.43(2)(a)), or
- an agreement with any government agency (federal, State or Territory) to exchange such information (cl.43(2)(e)).

The only limitation on these disclosures is that disclosures for the purpose of investigating or prosecuting an offence will not be allowed if the Minister first proactively prescribes a class of identifiers as not to be accessed or disclosed for these purposes (cl.42(5) and cl.43(3)).

Disclosures that would be allowed under this Bill would therefore include:

- a State or Territory police force, or any other body with investigative powers to collect information – under the law governing that other body
- Centrelink or the Tax Office – under an agreement, or under the social security or taxation legislation which allows widespread collections from other agencies
- a State driver licensing authority - under an agreement
- a person's employer, bank, video rental store or fitness club (each holds signatures, and potentially photographs) – for the purpose of data-

matching to identify a person

Our reading of this Bill is that there is nothing to prevent DIMIA from providing the biometric identifying information of every applicant for Australian citizenship to CrimTrac, which stores and shares fingerprints and other data on not only people convicted or even suspected of crimes, but increasingly also on 'innocent' people including victims of crime and relatives of missing persons.

In short, this Bill does nothing to prevent, and indeed goes a considerable way towards achieving, a national fingerprint database.

Suggested amendments to address these concerns

We strongly urge the Committee to consider the following amendments by way of measures to safeguard Australians (and those seeking to become Australians) from abuse of their personal information.

To limit collections of biometrics:

- amend clause 10 to delete paras (a) and (d), to delete the inclusion of fingerprints / handprints and iris scans, *or*
- amend clause 41 to insert a requirement that the Minister engage in further expert and public consultation prior to collecting any biometric identifiers other than signatures (i.e. before collecting fingerprints, handprints, or iris scans)

To limit any further expansion of the collection of biometrics:

- amend clause 10 to delete para (f), so that no new forms of biometric identifiers may be added simply by regulation, *or*
- amend clause 10(f) such that no additional forms of identifiers may be prescribed by regulation in the absence of further expert and public consultation

To limit secondary use and disclosure of biometrics:

- amend clause 42(2) to delete para (h)
- amend clause 43(2) to delete paras (a) and (e)
- replace cl.42(2)(a) with an exemption to allow verification of identifiers within a 'blind' system such as that proposed for the national Document Verification System (i.e. in such a way as to not disclose details of the query to any other person, agency or body, in which the query result comes back as 'yes' or 'no')

By "expert and public consultation" above we mean commissioning and publishing an independent Privacy Impact Assessment and then seeking further public submissions.

Again I apologise for the brief nature of this submission. We would be pleased to address any queries arising from this submission.

The Australian Privacy Foundation is pleased to have its submissions published as a matter of course.

Yours sincerely,

Anna Johnston
Chair, Australian Privacy Foundation

Phone: (02) 9432 0320

About the Australian Privacy Foundation

The Australian Privacy Foundation is the leading non-governmental organisation dedicated to protecting the privacy rights of Australians. The Foundation aims 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. For further information about us see www.privacy.org.au