



**Australian
Privacy
Foundation**

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

Human Services (Enhanced Service Delivery) Bill

Exposure Draft of December 2006

http://www.accesscard.gov.au/exposure_draft.html

Australian Privacy Foundation submission to the Department of Human Services, Office of Access Card

12 January 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 organisation, see www.privacy.org.au

Introduction

The APF has previously expressed very serious concerns about many aspects of the Government's proposal to introduce an Access Card because, in its present form, and despite the Government's statements to the contrary, the proposal is indistinguishable from a national identification scheme.

This Submission relates solely to the Exposure Draft of the Human Services (Enhanced Service Delivery) Bill 2007, made available on 13 December 2006.

The first section below contains comments on crucial aspects of the draft legislation that are of a more general nature. The second section provides submissions on more specific aspects.

General Comments

The process adopted by the Government is not an acceptable approach to the development of a proposal which has such extraordinarily grave implications for Australian society and democracy.

One key problem is that information is being dripped out in instalments. A great many important aspects of the regime have not been addressed to date. The result is that it is impossible to assess the complete package, or to see each aspect that has been announced in the context in which it is intended to exist.

The serious inadequacy of the information currently available is acknowledged in the Overview of the proposed legislative package (Section 8.9). Examples of vital omissions include effective oversight and governance of the access card system; dependants, carers and other linked persons; suspensions and cancellations of registration and the card; the need for, and use of, the card by persons overseas; replacement of lost and stolen cards; the interaction of the access card and existing cards during the transitional period between 2008 and 2010; protection of information; issues relating to and individual's area of the chip; computer hacking and other offences and inter-personal relationship with the Criminal Code; and requirements to present the card to obtain Commonwealth benefits from 2010.

Such aspects cannot simply be 'added on' at a later stage, but are inextricably linked to whether the proposed system will function in accordance with stated aims and whether it can meet appropriate privacy standards. For example, unless issues relating to dependants and carers are dealt with at the outset, there is no way of assessing whether the proposed legislation can deliver efficient and privacy-sensitive Medicare services to all of the Australian population.

Until draft legislation is provided on all issues central to the operation of the proposed Access Card, there is no meaningful basis on which to assess the proposal as a whole. It is therefore not appropriate to introduce any legislation until these matters have been dealt with, and consolidated into a complete legislative package for public assessment.

Another key problem is that DHS is not conducting a proper Privacy Impact Assessment (PIA), nor conducting proper consultations. The Task Force has been placed between DHS and the public. It functions as a buffer, shielding DHS executives and officers from the views of representative and advocacy organisations, watering down the comments made by them, and enabling the Department and Minister to pick and choose among the Task Force's recommendations. Any hope that public interest groups had that their comments and criticisms would be addressed were undermined when the Task Force's first set of recommendations were little more than empty 'motherhood statements', and demolished when the Minister diluted them even further.

One element of the inadequacies in relation to consultation was the Department's refusal to provide travel support to public interest organisations to enable them to be represented at the 'Consumer & Privacy Briefing' held on 13 December, in Sydney only. This resulted in many organisations being unable to be represented or being under-represented.

The APF submits that the Department cannot send this Bill forward at this stage. It must hold back the current tranche, construct a complete package of legislation, conduct meaningful consultations on the package as a whole, and finally take the amended package forward to the Parliament.

Specific Comments

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

1. 'Legal Name'

The APF submits that the very concept of a 'legal name' is foreign to Australian law, that it is an imposition that is demeaning and in any case unnecessary, and that it should be deleted from the proposal in its entirety.

2. 'Policy Statements'

The intent and the effect of cl. 30 are completely opaque. The clause purports to give a Minister powers to affect the interpretation, operation or scope of the law by uttering "a written statement of the policy of the Australian Government in relation to the administration of this Act". It appears, however, that many aspects of the legislation may be ambiguous, and that this clause may enable adjustments, which could make the scheme even more hostile to the Australian population or segments of it. It appears that such statements may not even be disallowable instruments.

The APF submits that the clause should be deleted, or clarified and tightened to avoid such an effect.

3. Delegations

In addition to the problem raised in the previous sub-section, a vast amount of the substance of the scheme is delegated to the Minister and the Department, through such expressions as 'approved by the Secretary' and 'that the Secretary determines', and the enormously wide delegations granted throughout Part 5. This appears to extend to such exemptions and exceptions not even being disallowable instruments.

The public does not trust the executive arm to be given such powers, and with good reason.

Any proposal that has vast implications for the Australian population must be complete, must be transparent, and must be explicitly authorised by Parliament.

The APF accordingly submits that all such language and delegations be removed from the many places they appear in the Bill.

4. The Information on the Register

Part 2 Division 3 ss. 70-90 would create a Register that is extraordinarily privacy-invasive, and is nothing less than the hub of a national identification scheme.

Under s.75 Item 1(d), the Bill would authorise the government to store any other names that it is aware that the person uses. This is highly intrusive, and appears to be completely lacking in any forms of control. This alone represents a very serious breach of public trust.

The data is extensible at the whim of the Minister and the Department, through weaknesses that have been contrived in such parts of the Bill as s.75, Items 6, 11, 13 and particularly 15. In the face of such loopholes, the assurances in s.90 are irrelevant.

No provision is made in relation to such seriously intrusive and dangerous items as residential address, with the single exception of protected witnesses under s.80(1)(a). This is a life-and-death issue for far more categories of people than just protected witnesses. Protections far more substantial and far better articulated than 'the Secretary must not include particular information' are essential, for protected witness and all other categories.

The data and the copies of so-called 'proof of identity' documents represent the raw materials needed for identity theft, and they would be stored in a single, centralised government repository. No government repository has, or ever can have, security features sufficient to preclude access to and use of such enormously valuable data for inappropriate uses and access, both by government and others.

In addition, the log-files would constitute an extraordinarily powerful person location and tracking tool, the likes of which should never be granted by any population to any Government.

The APF submits that under no circumstances should such an intrusive and insecure scheme be implemented, and that under no circumstances should such features be reflected in legislation.

5. The Personal Data in the Chip

The data stored in the chip is extensible at the whim of the Minister and the Department, through weaknesses that have been contrived in such parts of the Bill as s.160, Items 10 and particularly 15. In the face of such loopholes, the assurances in s.170 are irrelevant.

The 'card PIN' is stated to be encrypted. That is a completely inadequate security design, because it can be decrypted by any card-reader that has access to the decryption key, and by any organisation that acquires the data and has access to the decryption key. The appropriate design involves one-way hashing of the PIN, so that the card-holder is not exposed to masquerade by devices and organisations that have access to the decryption key.

The various identifiers either are already authorised to be in the chip (cl. 160 Items 11, 12 and 14) or are capable of being added to the chip by the Department, without so much as review by the Parliament (cl. 160 Item 10). This aspect alone dispels any doubts about whether this is intended as a national identification scheme.

Further, it appears that the card is not utilising separate secure zones, and accordingly every card-reader that has access to any personal data has access to all personal data. That is a completely inadequate security design.

The APF submits that under no circumstances should personal data as intensive and dangerous as this be stored in such a way on a chip on a card, and that under no circumstances should such features be reflected in legislation.

The APF submits that all identifiers must be accessible only by the organisations and in relation to the government programs for which they are the appropriate identifier.

The APF submits that under no circumstances should a security design as inadequate as this be implemented, and that under no circumstances should a security design as inadequate as this be reflected in legislation.

6. Ownership of the Access Card

In cl.175, the words "you own your own access card" purport to grant ownership of the card to the cardholder.

But this provision appears to bring with it no rights whatsoever, because all powers in respect to the data, the content of the data, the card's usage, and the card's ongoing usability remain with the Commonwealth.

The APF submits that the clause is empty, and hence misleading, and that it should be deleted.

7. Ownership of the Personal Data in the Chip

The Bill at cl.185 purports to confer on the Commonwealth ownership of the personal data in the chip.

This is a complete departure from established law, in that data is currently not the subject of property rights, although of course chattels on which personal data is recorded are.

The APF submits that, even if it were appropriate to overturn well-established law and create property rights in data, it is completely unacceptable to vest such property rights in personal data in any person other than the person to whom the data relates.

The APF accordingly submits that cl.185 either be deleted, or replaced with a provision that deals with interests not property rights, and that appropriately reflects the existence of interests on the part of the person to whom the data relates as well as the Commonwealth, and the critical importance of the interests of the person to whom the data relates.

8. Abuse of the Card

The provisions in cls. 210 and 215 relating to unauthorised persons requiring production of the card have been phrased so as to create many loopholes. For example, a card may be required to be provided for a purpose other than identification. In addition, a card may be merely requested, but benefits, services or concessions denied if the request is not satisfied. This aspect alone is sufficient to confirm the Foundation's view that this is a national identification scheme.

The APF submits that the offence provisions need to be completely re-worked, if the Government is actually sincere about its claim that the card's usage will be limited, or even if the Government intends it to be widely used but prefers that this not be obvious until after the scheme is operational.

In light of this problem, the provisions in cl.190 relating to use of the card by the card-holder for any lawful purpose also need to be re-considered.

9. Language

The term 'benefit' is paternalistic. It is justified in some cases, such as transfer payments in the forms of unfunded pensions and allowances, and grants. But it is not appropriate to use it to refer to payments that have been funded, or substantially funded, other than by the government.

Two examples of payments for which the term 'benefit' is inappropriate are:

- Medicare refunds
- payments passed via the Child Support Agency

Further, it is misleading, and possibly even demeaning, to refer to evidence of an attribute such as being a veteran or TPI as being in itself a 'benefit'. Such evidence may be used in support of an application for such benefits as a 'disabled parking sticker', but is not in itself a benefit.

The APF submits that the term 'benefit' should be reduced in its scope, and additional terms such as 'entitlements', 'payments' and 'evidence of attributes' should be added into the definitions and the body of the Bill.

Conclusions

The APF's very serious concerns about the Government's proposal to introduce an Access Card have been exacerbated by the large number of extremely serious defects that are apparent in the first Bill. The APF reiterates that, in its present form, and despite the Government's statements to the contrary, the proposal is indistinguishable from a national identification scheme. It is unacceptable for this Bill to proceed until the Government has placed the entire proposal on the table, so that the Australian public can see the full scope of what is proposed.

The APF contact in relation to this Submission is Nigel Waters, Policy Coordinator:
mail@privacy.org.au