Electronic Frontiers Australia Inc

PO Box 382 North Adelaide
SA 5006 AUSTRALIA
www.efa.org.au
email@efa.org.au
Tel: 07 3424 0201
Fax: 07 3424 0241

28 February 2007

Committee Secretary
Senate Finance and Public Administration Committee
Department of the Senate
PO Box 6100
Parliament House
Canberra ACT 2600

Email: fpa.sen@aph.gov.au

Dear Sir/Madam

Inquiry Into Human Services (Enhanced Service Delivery) Bill 2007

Please find attached submission from Electronic Frontiers Australia Inc. to the Committee's inquiry.

EFA appreciates the opportunity to make a submission and would be pleased to present oral testimony and respond to any questions Committee members may have. In the event that the Committee may wish to ask EFA to attend a hearing, with a view to assisting the Committee Secretariat in scheduling hearings, we advise that the most convenient (in view of our Executive Director's current appointment/meeting schedule) would be the hearing scheduled for Tuesday, or less preferred, Monday.

Yours sincerely

Irene Graham
Executive Director
Electronic Frontiers Australia Inc.

Electronic Frontiers Australia Inc. (EFA)
Submission

To: Senate Finance and Public Administration Standing Committee
Re: Access Card - Inquiry Into Human Services (Enhanced Service Delivery) Bill 2007

28 February 2007

Contents:

---

1. Executive Summary

a. The government's introduction of the *Human Services (Enhanced Service Delivery) Bill 2007* into Parliament is premature and inappropriate. In the absence of the other two proposed tranches of Access Card legislation, and absence of publicly available detail concerning the architecture and operational aspects of the chip and system, it is impossible to know the effect and potential ramifications of numerous provisions of the current Bill. Information concerning the architecture of the chip and related system is critical to the question of whether the public will be able to trust the system to secure and protect their personal information.

b. No Access Card legislation should be enacted until the government has publicly disclosed all details of the proposed system and the other two tranches of proposed legislation and there has been a significantly more appropriate length of time for public and Parliamentary scrutiny of such proposals than has been the case to date.

c. The Act should have a title that makes it readily apparent to the general public what the Act is about.

d. Government policy in relation to the administration of the Act should be determined and made apparent in the drafting of the Act, not determined from time to time by the Minister or anyone else. This provision appears intended to facilitate function creep and/or changes without Parliamentary or public scrutiny. At the least any such policy statement should be a disallowable instrument.

e. The definition of "document", in conjunction with the broad powers to be granted to the Secretary, would enable the Secretary to require that finger prints, iris scans, etc. be provided. The definition of "document" must be amended to exclude paper or "other material" on which there is any biometric information/data other than facial data.

f. EFA objects to a new concept of a "legal name" being introduced into Australian law. The registration of births, deaths and marriages legislation in every State and Territory of Australia states that it "does not prevent a change of name by repute or usage". The Commonwealth Government should not over-ride individuals' right to use such a name, nor force them to register under a different so-called "legal name".

g. If the legislation is to grant the Secretary the power to refuse to register a name on the grounds he/she is "satisfied" that use of the name is prohibited, the public and the Parliament should be informed by the government, before legislation is enacted, as to what laws of the Commonwealth, a State or a Territory exist that prohibit the use of a name. The public are entitled to know of the circumstances in which the Secretary could refuse to register a person for an Access Card, and hence prevent them obtaining Medicare refunds etc. on the grounds of use of a "prohibited" name.

h. The proposed definition of "inappropriate name" would ban names that may exist on birth certificates issued under the law of at least three of the States. If Commonwealth legislation is to copy definitions from State laws, it must use the least restrictive definition.

i. The extensive list of information about individuals that must be included in the Register, which goes beyond the government's previous statements on this matter, demonstrates that the Register is unquestionably intended to be a national ID database for the purpose of facilitating surveillance and monitoring of, and data matching in relation to, all citizens and other Australian residents.

j. It is astounding that the Explanatory Memorandum claims the unique serial number of a chip, to be included in the Register, is merely "technical or administrative information" and is not a personal identifier. The unique serial number is burned into the memory of a chip during manufacture. We understand that it therefore cannot be protected from disclosure by e.g. a PIN, and can be read by any ISO compliant card reader. Hence, this number is highly likely to become a unique national identification number. Moreover, the absence of any mention of this number in offence provisions strongly suggests that it is this unique number that the government intends be used as a national ID number.

k. The legislation should not grant the Secretary and the Minister the power, as contained in s17(1)17 and s34(1)17 of the Bill, to include other unspecified information in the Register and on the chip. Such powers render lists in s17 and s34 and the implied promises of s20 and s36 nugatory because the legislation does not clearly limit the information that can be placed on the Register, and on the card chip, without the individual's consent.

l. The Access Card number and individual's signature should not be mandatorily printed on the surface of the card for much the same reasons as the Fels Task Force recommended those two items not be printed on the card. Printing of number and signature on the surface of the card should be optional.

m. While it appears that, since the exposure draft, the Government has decided to cease attempting to take over ownership of citizens' names and other personal information, EFA nevertheless remains of the view that it is ridiculous for legislation to contend that individuals "own" the card given the many legislative restrictions in the Bill on what individuals may do to, with, and in relation to, the card.

n. A number of the offence provisions are largely illusory and/or suffer from a deficiencies and inadequacies resulting in loopholes.

o. The Bill must be amended to contain provisions over-riding section 10.5 of the *Criminal Code Act 1995* and any other provisions in existing law which provides an "excuse" or exemption from criminal responsibility in relation to the offences in the Bill. If there are to be exemptions to the offences in the Bill, these must be explicitly specified in the Bill.

p. EFA is strongly opposed to the criminal offence of changing 'information in the Commonwealth's area of the chip in your access card' on the grounds that (a) it demonstrates DHS has no confidence in the security of the chip architecture, (b) it is poorly drafted enabling criminal conviction of a person for conduct that the person did not intend, or know, would result in changes to information in the Commonwealth's area of the chip, and (c) it will deter legitimate investigation into whether or not the personal information on the chip is secure.

q. In our view s45(2) is a token offence - it is most unlikely to ever result in prosecution and conviction. While the explanatory material purports that this offence will provide protection for 'vulnerable' people, it seems unlikely that the prosecution, or the vulnerable person, could prove what the particular person ("you") understood to be meant to the standard of "beyond a reasonable doubt" as required in criminal law.

r. The factual basis of the offence of failing to give an access card to the Secretary immediately on demand appears to be created by no more than the Secretary's suspicion of particular conduct by the card holder or another person. EFA considers this to be a completely inappropriate basis for a criminal offence.

s. The use of the phrase "without reasonable excuse" in offence provisions shows that DHS knows that the width of the offence is too broad and believes that the potential for innocuous conduct to be caught by the offence is very great. Such offences should be re-drafted to significantly reduce the potential for innocuous conduct to be caught.

t. EFA has doubts as to the probability of enforcement of a number of the criminal offences, due to the nature of criminal law and the Prosecution Policy of the Commonwealth (which we do not criticise) and hence whether these criminal offences will afford adequate protection to individuals.

u. Where individuals suffer detriment, disadvantage, inconvenience, costs, etc, arising from breach of the Act by another person, a combination of a decision not to prosecute and no civil remedy available will not be satisfactory. EFA submits that civil remedies should be provided to enable the Federal Court of Australia or a court of a State or Territory, on the application of an aggrieved person, to grant the aggrieved person remedial relief.

---

2. Introduction

The government's introduction of the Human Services (Enhanced Service Delivery) Bill 2007[1] into Parliament is premature and inappropriate. In the absence of the other two proposed tranches of Access Card legislation, and absence of publicly available detail concerning the architecture and operational aspects of the chip and system, it is impossible to know the effect and potential ramifications of numerous provisions of the current Bill. Further, information concerning the architecture of the chip and related system is critical to the question of whether the public will be able to trust the system to secure and protect their personal information.

In view of the above, while this submission addresses numerous flaws and loopholes in the Bill, EFA is adamantly opposed to passage of the Bill whether or not all of the issues raised herein are adequately addressed and resolved. No Access Card legislation should be enacted until the government has publicly disclosed all details of the proposed system and the other two tranches of proposed legislation.

One of the major flaws in the Bill concerns the intention to store the unique serial number of the chip in the Register and that no prohibitions on copying, collection, use or disclosure of this number are contained in the Bill. The government has not provided any information as to the purpose of including this number in the Register - it is merely briefly mentioned in the Explanatory Memorandum. Furthermore it is astounding that the Explanatory Memorandum claims this unique number is merely "technical or administrative information" and is not a personal identifier. The unique serial number is burned into the memory of a chip during manufacture. We understand that it therefore cannot be protected from disclosure by e.g. a PIN, and can be read by any ISO compliant card reader. Hence, this number is highly likely to become a unique national identification number. Moreover, the absence of any mention of this number in offence provisions strongly suggests that it is this unique number that the government intends become a national ID number.

In relation to architecture and operational aspects of the chip and system, just one example of the lack of adequate information concerns the means of disclosure of a person's concession status to businesses and State Government agencies etc. The discussion about this matter during recent Estimates gives rise to a number of questions concerning, not only privacy protection, but the general practicality and technical feasibility of the claims made by DHS representatives. This matter is discussed under "Concession Status" later herein.

EFA remains opposed to the Access Card and related national ID database/system in its current form. Many of the issues and concerns raised in our submission to the DHS Access Card Consumer and Privacy Taskforce[2] in response to their Discussion Paper No. 1 remain current. Among other things, the government has not provided adequate justification for the amalgamation of Medicare cards and Centrelink cards into one ID card and we note that a considerable amount of information to be collected and stored relates to eligibility for Centrelink benefits not Medicare rebates. Hence the 5.5 million Australians who only have a Medicare are to be forced to provide information, for storage in a centralised identity database, that is not necessary for the provision of Medicare rebates. Amalgamation of these two different types of services onto one identity card, together with the establishment of a centralised identity database, are the core components of the Access Card system that make it completely unacceptable.

The Access Card in its current form is unquestionably a national identity card and we reject the government's claims that registration for the card is "voluntary". If the government intends to continue claiming the card is "voluntary", at the least it should amend taxation legislation to provide that during any financial year that a person has not "owned" an Access Card they are not required to pay the Medicare levy. It is entirely inappropriate to force citizens to pay taxation specifically to fund Medicare rebates and then refuse to provide them with rebates unless they "voluntarily" register with a national identification database.

EFA is not opposed, in principle, to the issue of smartcards by government agencies. Our position on use of smartcards depends on the particular model, after taking into consideration a range of matters including whether or not the model is appropriately adapted to serve a legitimate and justified purpose. The currently planned Access Card system does not pass this test.

---

3. Title of the Act

EFA considers the title of the proposed Act[3], i.e. "Human Services (Enhanced Service Delivery) Act 2007", to be bureaucratic newspeak. We are of the view that the Act should have a name that makes it readily apparent to the general public what the Act is about. We submit that it should be named the "Human Services (Health and Social Services Access Card) Act" and if that is not to be the name of the card, the title should contain the name decided on. The name of the card should be decided before legislation is enacted for the reasons put forward later herein.

---

4. Definitions

chip means a microchip or any other device that stores or processes information.

This definition should be amended to the type of microchip intended to be placed in the Access Card, or at the least limited to a contact chip/device. The proposed definition would permit the use of a contactless chip, which carries significantly greater security/privacy risks, without Parliamentary or public scrutiny and/or the use of any other 'device' with less effective security mechanisms than the type of chip which the government has stated will be used.

document includes:
(a) any paper or other material on which there is writing; or
(b) any paper or other material on which there are marks, figures, symbols or perforations that are:
(i) capable of being given a meaning by persons qualified to interpret them; or
(ii) capable of being responded to by a computer, a machine or an electronic device; or
(c) any article or material from which sounds, images or writings are capable of being reproduced with or without the aid of any other article or device.

This definition, in conjunction with the broad powers to be granted to the Secretary, would enable the Secretary to demand finger prints, iris scans, etc. be provided.

While we note that s17(1)17 concerning "other information" has been changed since the exposure draft to exclude "other" information that "identif[ies] you by name or other personal identifiers", this only prevents inclusion of such "other" information in the Register and on the chip. It does not prevent the Secretary from requiring, under s13(2)(b)(i) and s13(4)(a), an individual to provide a "document" containing fingerprints or iris scan etc, nor does it prevent the Secretary from storing such a document somewhere other than in the Register.

The definition of "document" must be amended to exclude paper or "other material" on which there is any biometric information/data other than facial data. If the government plans to require the provision of finger prints or iris scans etc either in the short or long term future, such plans should be required to be the subject of public and Parliamentary scrutiny.

legal name of an individual means:
(a) the name on a certificate, entry or record of the individual's birth, being a certificate granted or entry or record made by the Registrar of births, deaths and marriages (however described) of a State or Territory; or
(b) the name on the individual's Australian passport issued under the Australian Passports Act 2005; or
(c) the name on a certificate of citizenship granted to the individual under the Australian Citizenship Act 1948; or
(d) the name on a certificate, entry or record of the individual's marriage, being a certificate granted or entry or record made by the Registrar of births, deaths and marriages (however described) of a State or Territory; or
(e) the name included, by way of effecting a name change of the individual, on a register kept under a law of a State or
Territory by the Registrar of births, deaths and marriages (however described) of the State or Territory; or
(f) if none of paragraphs (a) to (e) apply to the individual—the name on a passport issued to the individual by a foreign country; or
(g) if none of paragraphs (a) to (f) apply to the individual—the name on a document prescribed by the regulations.
Note: For prescription of documents by class, see subsection 13(3) of the Legislative Instruments Act 2003.

The definition and information provided in the explanatory material concerning the new term "legal name" is inadequate and unclear.

Among other things, who will determine which of the names on the documents listed is an individual's "legal name"? This definition appears intended to give the government/DHS the power to decide what a person's name is instead of the person.

EFA notes that registration of births, deaths and marriages legislation in every State and Territory of Australia states that it "*does not prevent a change of name by repute or usage*". EFA objects to the Commonwealth Government over-riding the right and liberty of individuals under State and Territory law to use and be known by a name established by repute or usage.

EFA considers there are many questions required to be answered by the government prior to finalising and enacting any proposed legislation concerning "legal names". Such questions include, but are not limited to:

- In the case of a woman who is separated or divorced, and has chosen to re-establish her maiden name by repute or usage, will that name be permitted to be recorded as her "legal name" or will she be forced to have her married name recorded in the national ID database (Register), and on the chip in the card, because her marriage certificate is more recent than her birth certificate?
- Will the "legal name" be allowed to be changed at a future time when, for example, a person marries, or a person reverts to a previous name after divorce or death of the spouse, or changes their name by Deed? If so, what procedures will apply, i.e. how difficult will it be for an individual to have their "legal name" changed?
- How will highly sensitive issues pertaining to the name of transgender persons be dealt with? Will such persons be forced to have a "legal name" recorded (e.g. from their birth certificate) that indicates a sexual assignment that is *not* apparent from their photo and is not the name they use (established by repute or usage)?

EFA objects to a new concept of a "legal name" whether determined by the government or otherwise, being introduced into Australian law. Individuals should continue to be able to use, as a matter of general practice, the name they wish and DHS agencies should be required to respect an individual's preference, not force them to have a so-called "legal name" recorded in the national ID database (Register), nor on the chip in the card, from where it will be exposed to government agencies' staff and business entities' staff whenever the PIN pertaining to the Commonwealth area is entered.

Further, EFA submits that no legislation concerning names or registration requirements and process should be enacted until the Task Force has completed its public consultation on these matters and submitted its recommendations to government and such recommendations have been made public.

Missing Definition of "Commonwealth's area"

Although the term "Commonwealth's area" is referred to in numerous place in the Bill, the term is not defined. As this term is referred to in criminal offences we consider it important that it be defined and as clearly as possible. Criminal courts should not be left to attempt to determine what was intended by the government/Parliament. For example, is the "Commonwealth area" limited to the area containing information listed in s34, or is it intended to also include system software etc on the chip?

The user's/card holder's area may also require definition. However, we are not able to determine whether it will be important to define same in the absence of the proposed second and third tranche of this legislation.

---

5. Policy Statements

> *8 Administration of this Act to accord with Australian Government policy Policy statement*
> *(1) The Minister may, in consultation with the *DVA Minister, prepare a written statement of the policy of the Australian Government in relation to the administration of this Act. ...*

Government policy in relation to the administration of the Act should be determined and made apparent in the drafting of the Act, not determined from time to time by the Minister or anyone else. This provision appears intended

to facilitate function creep and/or changes without Parliamentary approval. At the least, any such policy statement should be a disallowable instrument.

The claims made in the Explanatory Memorandum ("EM") about the limitations of the Minister's powers in this regard do not reflect what is written in the Bill. If the government truly intends s8 to incorporate limitations referred to in the EM, the government ought not have any problem with writing same into the actual Bill.

Furthermore, EFA notes that a number of statements in the EM appear to be inconsistent making it impossible to comprehend the government's intent. As one example, in relation to "policy statements" (Section 8), the EM states:

> *This clause does not authorise the Minister to issue policy statements that ... would require officers administering the Act to make particular decisions. The provision is intended to allow the Minister to provide general high level guidance to the Secretary (and delegates) about matters relevant to the administration of the Bill.*

and with regard to exemptions in relation to eligibility for an access card (Section 22), the EM states:

> *It is intended that there will be internal administrative policy guidelines to provide guidance to delegates making decisions regarding exemptions.*

What is the purpose of requiring "policy statements" to be "tabled in both Houses of Parliament" given those will only contain "high level guidance" and there will also be "internal administrative policy guidelines".

EFA submits that **all** "policy guidelines" and "administrative policy guidelines" must be required to be tabled in Parliament and must be subject to disallowance.

Alternatively the government must establish its policy in relation to administration of the Act and set that out in an amended version of the Bill. Far too many important issues are being left to be resolved and implemented, without Parliamentary approval, at some future date.

---

6. Powers to demand/require and store information

6.1 Registration

13 Applying for registration
...
(2) For the purposes of paragraph (1)(a), a written application must:
(a) be in the form approved by the Secretary; and
*(b) be accompanied by such other specified information or specified *document that the Secretary:*
(i) determines is needed for the Secretary to be satisfied of your identity; or
*(ii) determines is needed to obtain information that is required to be included on the *Register.*
...
*(4) For the purposes of assessing your application, the Secretary may request you to give the Secretary specified additional information or a specified additional *document that the Secretary:*
(a) determines is needed for the Secretary to be satisfied that you are eligible to be registered; or
(b) determines is needed for the Secretary to be satisfied of your identity; or
*(c) determines is needed to obtain information that is required to be included on the *Register.*

The types of information and documents required for registration should be specified in the legislation, not left to the Secretary to determine, and identity guidelines proposed to be determined by the Minister should also be specified in the legislation.

These provisions should be deleted from the Bill and await completion of the Task Force's consultation on registration related matters and subsequent government decisions following the Task Force recommendations. The provisions should then be re-drafted in a manner that restricts the Secretary's powers to demand information to information specified in the legislation.

Further, as mentioned earlier herein, s13(2)(b)(i) and s13(4) together with the definition of "document" would enable the Secretary to require that fingerprint, iris scan, etc, information be provided. This should not be permitted. While we note that s17(1)17 concerning "other information" has been changed since the exposure draft to exclude "other" information that "identif[ies] you by name or other personal identifiers", this only prevents inclusion of such "other" information in the Register and on the chip. It does not prevent the Secretary from requiring, under s13(2)(b)(i) and s13(4), an individual to provide a "document" containing fingerprints or iris scan etc, nor does it prevent the Secretary from storing such a document somewhere other than in the Register. The definition of "document", or s13 and s23, must be amended to clearly exclude biometric information, other than facial data.

The remarks above also apply to s23(2) and s23(4) concerning "Applying for an access card" which contains similar provisions/powers to s13(2) and s13(4).

6.2 Information in the Register and in the chip

> *17 Information on the Register*
> *(1) Once you are registered, the Secretary must include on the *Register the information set out in the following table. ...*

> *34 Information in the Commonwealth's area of the chip in your access card*
> *(1) The Secretary must include in the Commonwealth's area of the *chip in your access card the *information set out in the following table. ...*

We observe that information that must be included in the Register goes beyond the government's publicity about the contents of the Register prior to the exposure draft, and the Bill reveals even more information to be mandatorily collected stored. This includes:

- the unique serial number of the chip in an individual's card. This is an additional unique identifier to be stored in the Register which was not mentioned in the government's initial publicity materials.
- any name that is known to the Secretary, including when the individual has not provided that name and does not know that the Secretary knows it. This demonstrates that the Register is unquestionably intended to be a national ID database for the purpose of facilitating surveillance and monitoring of, and data matching in relation to, all citizens.
- whether or not a person is an Australian resident. This further confirms the national ID database intention. The Bill also adds "and such other information about that fact as is determined by the Secretary" although it is entirely unclear what other information about a person's residency status may be included.
- "postal address" (in addition to residential address). This also further confirms the national ID database intention.
- the country of origin of a person who is a visitor to Australia, where that country has an international agreement with Australia under the Health Insurance Act 1973, and the Secretary decides to include that information. This further confirms the national ID database intention. (This was not in the exposure draft).
- whether a person's proof of identity is, according to the Secretary, "full" or "interim". This was not in the exposure draft and the EM provides no information concerning the effect or purpose of this concerning whether individuals who have "interim" status will be denied services or may be otherwise discriminated against by government agencies and businesses.

None of the above information should be permitted to be stored in the Register, unless the individual explicitly and voluntarily requests that it be so stored.

Unique serial number of the chip

EFA has major concerns about the proposed inclusion of the unique serial number of the chip on the Register, especially in the apparent absence of any provisions designed to ensure this will not and cannot be lawfully used as a personal identifier for data matching, tracking, surveillance, and/or any other similar purpose.

In the above regard the Explanatory Memorandum states in relation to s17(1):

"Under item 17(a), the Secretary will be able to add technical or administrative information to the Register (for example, audit logs or the serial number of the chip).
Item 17(a) makes it clear that under this item the Secretary is not permitted to include any personal information that could identify a person by name or other personal identifier on the Register. Additionally, even the technical or administrative information that may be included under this item must be reasonably necessary for the administration of the Register or an access card."

Notwithstanding the above claims, the serial number of the chip is of itself a personal identifier - it will be linked with the person's name and other personal information in the Register and on the chip.

The unique serial number of a chip is burned into the chip memory by the manufacture of the smart card/chip. As such, it is our understanding that it is not technologically possible to protect it from disclosure when the card/chip is placed in a reader, i.e. it cannot be protected from disclosure by a PIN etc. This appears to be confirmed by, for example, the FAQ about smart card readers[4] on the site of Software House, a supplier of smart card readers, which states:

> "What is a smart card serial number? Is it encrypted?
> Each smart card contains an integrated chip with a unique permanent identification (UID) number burned-in during the manufacturing process. This UID is often referred to as the Card Serial Number (CSN). The card serial number is not encrypted and any reader that is ISO compliant can read the card serial number."

Hence, unless the Bill includes prohibitions on copying, use, etc of the card serial number number (which it does not), all other offences intended to prevent the access card number from becoming a national ID number will be meaningless, because the unique card serial number will be able to be used instead.

EFA notes that a card/chip will remain valid for a period of 10 years. If the government does not want a potentially large number of cards to be frequently lost, it seems the government may be well advised to implement prohibitions on collection, use and disclosure of the unique card serial number. (The provisions of the *Privacy Act 1988* are not adequate in the regard, and in any case do not apply to all business entities nor to State/Territory Government agencies.)

Audit logs

EFA questions what is meant by the reference in the Explanatory Memorandum to "audit logs" being "other information" that the Secretary may include on the Register.

Does this mean that when a card is docked in a reader that is linked to the Register (e.g. via the EFTPOS or some other communications system) for the purpose of checking concession status or any other reason, a record of the use of the card will be logged? If so, this raises significant privacy concerns. As pointed out on ABC Background Briefing[5] recently in relation to the proposed U.K. ID card:

> "*But what's perhaps most ominous about the proposal is that every time you formally check someone's identity using the identity card, more than just looking to see if the photo looks like the person who's presenting it, if you formally check the card, a record is kept on the national identity register in the form of an audit trail, saying 'On this particular occasion this institution or this organisation checked the identity of that particular person.' So if you open a bank account, they check your identity card, a record is kept 'On this particular occasion this bank checked or verified this person's identity.' So potentially forming a fairly detailed list of all the times that your identity was verified, and potentially also allowing checking whose identity was also verified at the same location at around about the same time. So you could get patterns of who had registered, you're using it to check IDs for going into a bar, then you could see who else was in the bar at the same time, which has the potential for being misused and drawing inferences that perhaps are inappropriate.*"

The potential for tracking and surveillance of citizens is one of the reasons EFA is opposed to a centralised database being linked to cards. If the smart card chip is secure, there ought not be any need for communication with a centralised database. If the card chip is not to be secure, such cards should not be implemented.

Names (Legal, Preferred and "Other")

The plan to store names in the Register that an individual has not provided, but are "known to" the Secretary, is totally unacceptable and must be deleted (s17(1)(d)). Apart from the privacy invasiveness of such a plan, it presents significant potential for incorrect and/or out of date information about an individual to be stored.

The information in the Bill and Explanatory Memorandum concerning the circumstances in which so-called "legal name" and/or preferred name will be included on the Register and/or on the chip in the card is confusing and hence unclear. The Bill appears to state that the Register will only contain the "legal name" unless either:

- the person is exempted under s65 from providing their legal name, or
- the person requests their preferred name also be included in the Register (in addition to their legal name).

However, the card chip is required to contain both the legal name ("protected by the personal identification number") and also the preferred name.

This appears to result in a situation whereby the name on the chip visible without PIN entry will not match the name on the Register (when an individual did not want/request their preferred name to be included on the Register). EFA questions what systems/procedures will be in place to ensure individuals are not accused of using a fake card etc when, for example, the card reader in the relevant office is defective/inoperative and the (preferred) name on the face of the card does not match the (legal) name in the Register, and/or when the person has forgotten their PIN and the name on the chip does not match the name in the Register.

Further, these provisions appear to make a mockery of the claims that a person will be able to use their preferred name for dealings with government agencies because they will apparently not be able to do so without agency staff knowing their "legal name" from the Register, and any other name that the Secretary knew although the individual did not provide it.

There is no justification for storing more than one name in relation to an individual unless an individual so requests (other than for the purposes of a national identity database and related citizen monitoring and tracking systems). The Access Card is said by government to be the means by which a DHS government agency can know that the card holder is entitled to a benefit. Once the Access Card is issued and is thereafter required to be used to prove to a DHS agency who the person is, it is irrelevant how many names the person may have or have had. Further, the government has stated that the reason/justification for requiring photograph and use of facial recognition technology is to prevent a person from registering twice, hence how many names they have or have used in the past is irrelevant.

Address

We observe the card chip is to contain only the residential address but the Register "must" also contain the postal address. We see no legitimate reason why the Register must contain a person's postal address unless the person so requests. Further, we question whether the system will be capable of ensuring a postal address is not downloaded to the card chip when an individual does not want that information on the chip.

Other Unspecified Information

The legislation should not grant the Secretary and the Minister the power, as contained in s17(1)17 and s34(1)17 of the Bill, to include other unspecified information in the Register and on the chip. Such powers render lists in s17 and s34 and the implied promises of s20 and s36 nugatory because the legislation does not clearly limit the information that can be placed on the Register, and on the card chip, without the individual's consent. Such powers result in the situation whereby citizens will not know what information about them is or may be included in the Register at any point in time (without regularly requesting such information under the relevant IPP).

If the government wishes the public to trust the government in relation to Access Card system, it ought not provide its Ministers and departmental staff, nor any future government's, with powers to include other unspecified information. At the least, the Secretary's proposed powers to include "other information" should be deleted from the Bill, so that the only "other information" that may be included must be determined by Minister, by legislative instrument and hence be disallowable.

While the Secretary's powers in the above regard may appear to have been narrowed since the exposure draft and to now concern, according to the Bill, "technical or administrative information", the lack of publicly available information about the government's "administrative policy" intent, and "administrative guidelines", etc. (as discussed earlier herein) gives rise to serious concern as to what type of information the government or the Secretary may regard as being "administrative" information.

Quite plainly the above can include personal information. The EM states that "*determinations by the Secretary under items [17(1)] 2, 3, 7, 8, 9, 12 and 17(a) only relate to technical or administrative matters*". However, those items provide the Secretary with power to determine whether or not particular types of personal information will be included in the Register. For example, item 2 is date of birth, item 3 is citizenship status, etc. Accordingly it seems clear that item 17 provides the Secretary with unlimited powers to include other personal information as well, notwithstanding the Bill contends it is "administrative" information.

It is also of major concern that the so-called "technical or administrative information" includes the unique serial number of the chip in an individual's access card, as discussed earlier herein.

Storage of scanned copies of birth certificates etc

The intention to scan copies of birth certificates, and other core identity documents, and store same in the Register database poses a totally unacceptable security risk. This intention together with the extensive list of information about individuals that will be included in the database puts beyond any doubt that the "Register" will be a national ID database and an extremely attractive honeypot for identity thieves because it will contain all information necessary to steal a person's identity, including information (on e.g. birth certificates) such as mother's maiden name which is commonly used by some banks and other businesses for the purpose of ascertaining identity during telephone calls.

Information about benefit cards

The Bill states that information which must be included in the Register includes information "about" any "benefit cards" that a person holds. Firstly, this aspect is incomprehensible in the context of government claims that the Access Card would replace 17 cards which include the cards defined as "benefit cards" in the Bill. Will the Access Card replace such cards or will individuals continue to be required to "hold" such cards (as the Bill indicates)? Secondly, inclusion of information about such cards shows that government claims that information pertaining to agencies will be kept separate from the Register are not true because the legislation explicitly enables such information to be included in the database. Medicare card numbers and benefit card numbers should not be permitted to be stored in the Register database at any time, nor should any information "about" such cards unless an individual so requests.

Gender / Sex

> *s17(1) and s34(1):*
> *~~gender - your gender;~~*
> *sex - your sex;*

EFA questions why the above change has been made since the exposure draft and whether or not the personal privacy of transgender people has been taken into account in a manner that will prevent invasion of their privacy by government agency staff and any other persons who have access to the Register and/or the content of the chip.

Card PIN

> *s34(1)*
> *9 card PIN etc.*
> *(a) if there is a personal identification number for your access card-that number, protected by encryption or other technological protection measure;*
> *(b) if there is other information (for example, a password) for authenticating your identity-that information, protected by encryption or other technological protection measure;*

Will card holders have to remember both a PIN and a password?

Significantly more information needs to be made publicly available about the architecture of the chip and related card readers etc. To date information released, together with the Bill, suggests the design of the chip will not provide adequate security and privacy of information on the chip.

While the Bill refers to a PIN in the Commonwealth area of the chip, it appears that very little of the information in the Commonwealth area will be protected by a PIN. In this regard, section 34 states that the following information on the chip will be protected by the PIN:

- your legal name

Will any other information on the chip be protected by the PIN, and if so, why is that not also stated in section 34?

Also of concern is that the Bill makes no reference to a PIN in the card holder's area. Therefore apparently information stored in the card holder's area of the chip will be viewable by government agency staff and other people when a card is placed in a card reader. Such a design is completely insecure and unacceptable.

Further, while we observe that the procurement document issued on 8 January 2007 states that "Card holders can choose to protect information in either area using a PIN", the apparent plan to have only one PIN appears to result in information in the card holder's area of the chip being viewable by other people when the PIN is entered for the purpose of providing access to protected information in the Commonwealth area. Such a design would be completely unacceptable.

Concession Status

EFA considers the discussion about access to information about concession status during Estimates hearings on 16 February 2007[6] raises a number of serious issues and questions.

Firstly, the DHS representative's reference to "our design idea" seems to show that it is currently unknown how concession information can be disclosed to e.g. cinemas offering discounts while also protecting the privacy and security of other information on the chip.

Secondly, the statement that "*We would be using the chip to indicate their concessional status and then using the EFTPOS system to simply identify that the person is concessional*" appears to show that in order to find out whether a person is currently entitled to concessions/discounts, the chip will communicate with the back-end centralised database. This enables tracking and recording, in the centralised government database, of every use of a card for obtaining a discount or concession.

Thirdly, it was stated that "*we are interested in personal card readers that could also achieve the same thing*". If a personal card reader, that is not connected to the EFTPOS system and back-end database, is to be used by e.g. cinema staff, bus drivers, etc. and be able to read the concession status (which may or may not be current) from the chip, then ensuring that the chip will only expose, e.g. "C" for concession, appears to be dependent on the card reader, that is, what particular commands the card reader sends to the operating system on the chip. As the Bill indicates there is to be only one PIN applicable to the "Commonwealth area" of the chip, entering that PIN into an "ordinary" card reader would expose not only concession status but all information in that area of the chip. Hence it appears that readers intended to be used for access only to concession status cannot be just "ordinary" readers, but will need to have special software provided by the government installed in the readers. (Such readers are sometimes referred to as "authorised readers", or "specially designed readers" as referred to in the KPMG document - they are not the same as those currently in premises such as Australia Post). If this is not to be the case, how can the public be assured that docking a card in a reader will only display e.g. "C"? In any case, even if Commonwealth government provided software is to be installed in readers in business and State Government premises and carried by bus drivers, etc, how will an individual be able to know/be assured that a card reader is only able to obtain that particular item of information? Individuals will have no idea what software is installed on any particular card reader.

EFA continues to be of the view that the total lack of information about how the chip and system will operate requires far too much blind trust on the part of the public and the Parliament. No legislation should be enacted prior to such time as the Government is able to publicly issue information significantly more detailed than consisting of a "design idea".

Death

We observe that s17(1)(14) implies that the information about dead people will be kept on the Register for ever. Surely cards 'owned' by persons who have died should be cancelled and information about them deleted within a reasonable period. This is another aspect that indicates the Register and the card have more to do with national identity documents and schemes than access to government benefits.

> *18 When Secretary may not include information on the Register*
> *(1) Despite subsection 17(1), the Secretary must not include particular information about you on the *Register under that subsection if:*
> *(a) the Secretary considers it would be inappropriate to do so because of your inclusion in the National Witness Protection Program; or*
> *(b) to do so would be inconsistent with a Commonwealth law.*
> *(2) Despite subsection 17(1), the Secretary must not include your preferred name or other name on the *Register if the Secretary is satisfied that use of that name is prohibited by a law of the Commonwealth, a State or a Territory.*
> *(3) Despite subsection 17(1), the Secretary may refuse to include your preferred name or other name on the *Register if the Secretary is satisfied that the name is an *inappropriate name.*

Exceptions

With regard to s18(1), in view of the vast amount of information to be included in the Register and resultant security risks, special provisions should not be limited to witnesses. Various other types of people will also be subject to an exceptionally high level of risk, including but not limited to, battered spouses, victims of stalkers, law enforcement officers under deep cover, etc.

Prohibited Names

With regard to s18(2), EFA is unaware of any provisions in Australian law that prohibit an individual from using as a matter of general practice any name they wish. Further, the registration of births, deaths and marriages legislation in every State and Territory of Australia states that it "does not prevent a change of name by repute or usage".

In addition, EFA sees no legitimate reason why an individual should be prevented, by Commonwealth law, from using a name that is prohibited by a law of a State or Territory in which the individual was not born and/or does not reside. The Bill should be amended to ensure such prohibition can not occur. Moreover, if the Secretary is to have this power, the public and the Parliament should be informed by the government, before legislation is enacted, as to what laws of the Commonwealth, a State or a Territory exist that prohibit the use of a name, so that the public and Parliament can know of the circumstances in which the Secretary could refuse to register a person for an Access Card, and hence prevent them obtaining Medicare refunds etc. on the grounds of use of a "prohibited" name. The foregoing remarks also apply to s30 concerning the preferred name a person wishes to have printed on a card.

Inappropriate Name

With regard to s18(3), we observe this enables the Secretary to refuse to include an "inappropriate name" on the Register which is defined as:

> *inappropriate name means a name that:*
> *(a) is obscene or offensive; or*
> *(b) could not practicably be established by repute or usage:*
> *(i) because it is too long; or*
> *(ii) because it consists of or includes symbols without phonetic significance; or*
> *(iii) for some other reason; or*
> *(c) includes or resembles an official title or rank; or*
> *(d) is contrary to the public interest for some other reason.*

The EM states "*This definition is based on a similar provision in the New South Wales Births, Deaths and Marriages Registration Act 1995 which prevents registration of prohibited names. Similar provisions apply in other States and*

Territories".

However, the NSW legislation is more prohibitive than the "similar" laws of several other States e.g. Victoria, South Australia and Western Australia.

EFA submits that, at the least, the definition to be used in Commonwealth law must use the least restrictive definition in State/Territory laws in order not to prohibit names that exist on certificates issued by States with less restrictive laws than NSW.

However, whether the above change is made or not, EFA objects to the government legislating to enable the government or the Secretary to prevent an individual from using as a matter of general practice any name that has been established by repute or usage. Reference to "inappropriate names" should be deleted from the Bill. If use of a particular name is not already prohibited by a law of the Commonwealth, a State or a Territory, it most certainly should not become prohibited by enactment of access card legislation.

19 Temporary information on the Register
*If you own an access card, the following *information may be temporarily included on the *Register until it is transferred to the Commonwealth's area of the *chip in your card:*
*(a) if you have a *medicare number-that number;*
*(b) if you have a *Reciprocal Health Care Card-the number of that card;*
(c) if DVA has allocated you a DVA file number-that number;
*(d) if you hold a *DVA White Card and you have a condition 24 that has a code under the *International Classification of 25 Diseases—that code.*

While the Section 19 has been changed slightly since the exposure draft (s85), it continues to be misleading and appears to be an attempt to imply to the general public that this information will not normally be held in the national ID database (Register).

However, Section 17(1)7 makes clear that the Secretary must include the above information on the Register on a permanent, not temporary, basis. This is further confirmed by the Explanatory Memorandum which states:

> "*Information about a benefit card held by an individual will be listed in the Register (see item 7 of the table in clause 17) and in the Commonwealth's area of the chip in the individual's access card (see item 10 of the table in clause 34). This is to ensure that relevant benefits or concessions will only be provided to those individuals who are entitled to the benefit or concession.*"

EFA fails to see why this information needs to be stored in Register, unless the Register database is going to be accessed by doctors, chemists, Medicare staff, Centrelink staff, cinema staff and other businesses' staff, etc, "to ensure that relevant benefits or concessions will only be provided to those individuals who are entitled to the benefit or concession."

EFA once again questions the purpose of storing information on the chip, if staff of agencies and businesses are to be required, or able, to access information in the Register. Statements in the EM strongly indicate that the foregoing will be the case. In relation to s17, it states:

> "*The information in the Register will be verified and will be able to be checked against cards that are presented by individuals when they claim benefits or seek services.*"

Currently, all indications are that the principal purpose of the Register is to be for use as a tracking and surveillance system pertaining to all usages of the card.

Unless Section 17(1)7 is changed, Section 19 regarding so-called "temporary information" should be deleted because it is apparently not factual and hence is misleading.

25 When Secretary issues you your access card
The Secretary is taken to have issued you your access card when:
(a) the Secretary sends your access card to you by post, or such other method as the Secretary determines; or

(b) you collect your access card from a place determined by the Secretary.

Clause (b) above should place an obligation on the Secretary to ensure any such "place" is convenient to the relevant individual.

EFA considers the intention to sent access cards "by post" highly insecure and recalls that many passports sent by post were lost and/or stolen when such a delivery method was used by the passport office. Given the probably high level of inconvenience to individuals if their access card is lost or stolen in transit by post, a more secure method of delivery is necessary.

27 Name, symbol and form of an access card
(1) The access card is to be known as the Health and Social Services Access Card, or such other name as the Minister determines in writing.
...
(4) An access card is to be in such form as the Minister determines in writing. ...
(5) A determination under subsection (1), (2) or (4) is not a legislative instrument.

The name and "form" of the access card should be established before legislation is enacted and specified in the legislation. Given use of the name in various circumstances is to be a criminal offence, the particular name should be readily findable in legislation (not merely made public in a newspaper advertisement as proposed in the Bill). Further, what is meant by the "form" of an access card is entirely unclear. Information on the meaning of the term "form" in this context should be made public and defined in the legislation.

6.3 Information on the surface of the card

30 Information on the surface of your access card
1 name ...
2 card number your access card number
...
5 signature

Comments earlier herein concerning "legal name" and on s18 concerning the Secretary's powers and prohibited and inappropriate names also apply to s30.

EFA is opposed to the card number and signature being mandatorily printed on the surface of the card for much the same reasons as the Fels Task Force recommended those two items not be printed on the card.

The government's argument that the number needs to be printed on the card so that persons who ring Centrelink etc can readily see and quote the number does not justify mandatory inclusion of the number on the surface card. Many of the 5.5 million people who only have a Medicare card would rarely if ever need to telephone Medicare. Further, many people already have numerous PINs and passwords and have developed personal means of remembering and/or securely storing such information. Individuals should not be forced to have the number printed on the Access Card merely because it would be convenient to some other people. Printing of the access card number on the card should be optional.

EFA does not agree with the Government's view (in the response to the Task Force recommendations) that "a digitised signature on the card provides greater utility and security for the cardholder". EFA considers the signature increases security risks and that individuals should be allowed to decide for themselves whether or not a signature on the card would provide them with "greater utility". Printing of the signature on the card should be optional.

6.4 Information in the Commonwealth's area of the chip

34 Information in the Commonwealth's area of the chip in your access card

The provisions of s34 are discussed in conjunction with those of s17 earlier herein.

7. Purported Card Ownership

Division 5—Ownership of your access card
37 You own your access card.
(1) You own your access card.
(2) You acquire ownership when your access card is issued to you (see section 25).

38 Ownership of intellectual property etc. in your access card
However, subsection 37(1) does not
*give you ownership of any intellectual property or *information that, at any time, is on the surface of, or in the *chip in, your access card that you would not otherwise have.*

39 What you cannot do with your access card
Despite subsection 37(1), you cannot sell your access card, or otherwise transfer any part of your ownership of it.

EFA observes that an equivalent of s185 of the exposure draft does not appear in the Bill and hence it appears the Government has decided to cease attempting to take over ownership of citizens' names and other personal information.

Nevertheless, EFA continues to be of the view that it is ridiculous for legislation to contend that individuals "own" the card given the many legislative restrictions in the Bill on what individuals may do to, with, and in relation to, the card.

Further, EFA observes that the proposed legislation states that an individual will acquire "ownership" of the card prior to the time the individual has possession of the card (see s25 as referred to in s37(2)). We question who will be responsible for the cost of replacement/re-issue of a card. Will the individual who "owns" the card be required to pay the cost of replacement/re-issue of their "lost property" either when it lost or stolen when sent to them "by post", or in any other circumstances?

EFA submits that references to ownership should be deleted. The legislation should grant rights to individuals in relation to use of the card they hold, instead of purporting to grant ownership and then creating criminal penalties to restrict what individuals are permitted to do with their own "property".

---

8. Requirement to carry card

42 No requirement for you to carry your access card
You are not required to carry your access card at all times.

At which times, or under what circumstances, will individuals be required to carry their card? If the government actually intends none, then the above should be changed to "You are not required to carry your access card at **any** time.", otherwise it should state the times/circumstances when individuals will be required to carry the card.

---

9. Offences

The proposed criminal offences in the Bill provide inadequate protection because a number of them are unlikely to be enforced and/or enforceable and some are largely illusory due, for example, to the operation of other legislation. In the foregoing regard, the Explanatory Memorandum states:

> "*For example, an authorised person who copied a person's access card number for a reason that was not connected with the provision of Commonwealth benefits would commit an offence under clause 57, unless that copying was with the card owner's written consent or* ***was excused under section 10.5 of the Criminal Code Act 1995 (which would enable copying if that was justified or excused by or under a law).***
> ...
>
> *Section 10.5 of the Criminal Code provides that a person does not commit an offence under a Commonwealth law if the person's actions are justified or otherwise excused under a law of the Commonwealth. For example, under section 108 of the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 reporting entities are, in certain circumstances, required to make and retain a copy of a document used for identification purposes.*
>
> *In a situation where a person chooses to provide their access card to a reporting entity (e.g. a bank), the entity would in certain circumstances be required under the Anti- Money Laundering and Counter-Terrorism Financing Act 2006 to make and retain a copy of the card (which would include the card number).* ***In this situation section 10.5 of the Criminal Code would apply and the reporting entity would not be criminally responsible under clause 57.***" [emphasis added]

The above shows the illusory nature of the offence prohibiting copying etc. Individuals who choose to show their Access Card to a person/entity will have no practical means of knowing whether that person is "excused" from the prohibition on copying, etc, without written consent.

Furthermore, in addition to existing laws providing an "excuse", this situation enables the current, or a future, government to introduce new legislation unrelated to the Access Card which has the effect of authorising/excusing copying etc of information on the Access Card without making that fact readily apparent to members of the Parliament or the public. Obviously this is a means of enabling function creep.

EFA submits that the Access Card Bill must contain provisions over-riding section 10.5 of the Criminal Code Act 1995 and any other provisions in existing law which would provide an excuse or exemption from criminal responsibility in relation to the offences in the Bill. If there are to be exemptions to the offences in the Bill, these must be explicitly specified in the Bill.

45 Requiring production of an access card for identification
(1) A person commits an offence if:
(a) the person requires you to produce your access card or someone else's access card; and
(b) the person does so for the purposes of identifying you or someone else; and
*(c) if the person is a *delegate or an *authorised person-the requirement is not made for the purposes of this Act; and*

(d) if the person is not an authorised person-the requirement is not made to establish that:
*(i) you hold, or someone else holds, a *benefit card; or*
*(ii) you have, or someone else has, a *medicare number.*

The offence should also prohibit requiring provision of an access card number, not only production of the actual card.

Furthermore, (d) should be limited to circumstances where the requester has a legitimate need to know that information. We gather the exception is intended to apply for example to doctors and chemists who have a legitimate need to know whether a person has a Medicare number, or a service provider offering discounts to pensioners, etc, but the exception is not limited to such persons with a legitimate need to know. It apparently allows any person at all to require production of an access card for the purpose of finding out whether a person has another card or number referred to in (i) and (ii).

We also question the reason for deletion of "or a Medicare card" from offence provisions given that the definition of "benefit card" does not (as it should not) include a Medicare card (except in relation to a small class of specified eligible persons who have time-limited Medicare cards). Reference to a Medicare card must be included to ensure the offence cannot be skated around by someone claiming to require production of a Medicare card to establish that another person holds Medicare card, not whether they have medicare number. This also applies to other offences where the reference to Medicare card has been deleted since the exposure draft.

45(2) A person commits an offence if:
(a) the person makes a statement (whether orally, in writing or any other way) to you that you could reasonably understand to mean that you are required to produce your access card or someone else's access card; and
(b) the person does so for the purposes of identifying you or someone else; and
*(c) if the person is a *delegate or an *authorised person—the requirement is not made for the purposes of this Act; and*
(d) if the person is not a delegate or an authorised person—the requirement is not made to establish that:
*(i) you hold, or someone else holds, a *benefit card or*
*(ii) you have, or someone else has, a *medicare number.*
Penalty: Imprisonment for 2 years or 120 penalty units, or both.

Section 45(2) suffers from the same defects and inadequacies as outlined in relation to Section 45(1) above.

Moreover, in our view s45(2) is a token offence - it is most unlikely to ever result in prosecution and conviction. While the explanatory material purports that this offence will provide protection for 'vulnerable' people, it seems extremely unlikely that the prosecution, or the vulnerable person, could prove what the particular person ("you") understood to be meant to the standard of "beyond a reasonable doubt" as required in criminal law. We also have some concerns about the appropriateness of requiring such vulnerable people to appear in a criminal court and be subjected to cross examination in relation to attempts to prove what they did or did not understand. Such a prospect is likely to further reduce the probability of prosecution. It may be more appropriate such an offence to refer to what "a reasonable person" would reasonably understand.

46 Requiring production of an access card for supply of goods and services etc.
(1) A person commits an offence if:
(a) the person requires you to produce your access card or someone else's access card; and
(b) the person does so in connection with a matter referred to in subsection (3); and
...
(2) A person commits an offence if:
(a) the person makes a statement (whether orally, in writing or any other way) to you that you could reasonably understand to mean that you are required to produce your access card or someone else's access card; and
(b) the person does so in connection with a matter referred to in subsection (3); and

Section 46 suffers from the same defects and inadequacies as outlined in relation to Sections 45(1) and 45(2) above.

In addition, we consider offences should apply to requiring production of the card or provision of the card number for any purpose whatsoever other than the purposes of the Act. It should not be limited to "supply of goods and services" nor should it be limited to a specified list of matters. EFA is not persuaded that the list of matters in proposed s46 would cover all circumstances in which individuals could be required to provide the card for purposes such as proving an address or date of birth or any other information about themselves and we consider it impractical if not impossible to attempt to produce such a list that would be adequate for the long term. The offences should apply in relation to all purposes other than the purposes of the Act.

Further, the offences do not deal with situations where the card or card number is requested, but not required, but benefits or goods or services are denied when the card holder declines to provide the card in response to a request for it. If the government is serious about the card not becoming a defacto national ID card, offences need to be established to strongly discourage discrimination against individuals who decline to provide their card or card number in response to a request for it. This situation is not covered by the proposed criminal offences and given the standard of proof in criminal law it is unlikely that 'requirement' would be interpreted to include 'request' and doubtful that a request could be proven to be in fact a requirement.

52 Changing information in the Commonwealth's area of the chip in your access card
*You commit an offence if you change any *information in the Commonwealth's area of the *chip in your access card.*
Penalty: Imprisonment for 2 years or 120 penalty units, or both.

EFA is strongly opposed to the above proposed offence on the grounds that (a) it demonstrates DHS has no confidence in the security of the chip architecture, (b) it is poorly drafted enabling criminal conviction of people who did not intend to change information, and (c) it will deter legitimate investigation into whether or not the personal information on the chip is secure.

Such an offence should not be necessary because the system architecture should designed so as to be trustworthy. It should ensure that information in the Commonwealth's area of the chip cannot be changed, either intentionally or accidentally, by unauthorised persons. The fact that such an offence has been deemed necessary raises major concerns about security (and reliability) of information on the chip. We observe that the Passports Act does not contain an offence pertaining to changing information on the chip in the passport. It appears that DFAT was confident about the trustworthiness and security of the architecture of their chip and related system but that DHS is not confident about the security of their chip and associated system architecture.

Moreover, if the chip and system architecture is not to be secure and trustworthy, there will exist the potential for unintended changes to be made to information Commonwealth's area of the chip when, for example, an individual is attempting to change the information in their own area, or as a result of use of a defective card reader/writer that was not known to be defective, etc.

Hence, it is of major concern that the construction of the proposed offence apparently enables criminal conviction of an individual for conduct that the person did **not** intend, or know, would result in changes to information in the Commonwealth's area of the chip.

In the above regard, the proposed offence applies the default fault element of intention to conduct, without regard to whether the person had any intention **to bring about the result** that information be changed. As pointed out in the Attorney-General's Department's Guidelines for framing Commonwealth offences "*it will almost always be clear that a person intended his or her own conduct*" and "*it is generally neither fair, nor useful, to subject people to criminal punishment for unintended actions or unforeseen consequences unless these resulted from an unjustified risk (ie recklessness)*".

EFA insists in the strongest terms that if such an offence is to remain (which should only be the case if DHS lacks confidence as to the security of their system), the offence must be re-drafted to ensure a person cannot be found guilty and punished for mere conduct, which resulted in unintended actions or unforeseen consequences etc. The offence must be amended to require proof of an additional physical element of result, to which the fault element of recklessness applies. For example, we are under the impression from the A-G Department Guidelines that the following construction would achieve that objective:

> 52 Changing information in the Commonwealth's area of the chip in your access card
> (1) A person commits an offence if:
> (a) the person engages in conduct; and
> (b) the conduct results in change to any *information in the Commonwealth's area of the *chip in your access card.

However, any offence pertaining to changing information would require exceptions, and may require specification of defences to minimise capture of innocuous activity.

For example, a person who changed the PIN on their access card would be guilty of the above offence as they would of the offence in the Bill. (EFA assumes and expects the system architecture will be designed so as to enable an individual to change their own PIN. Obviously it should not be an offence for an individual to change their PIN).

While the offence proposed above would be a significant improvement, EFA does not support the inclusion of such an offence. The system architecture should be secure and trustworthy. Moreover, the government should not introduce a criminal offence that can readily be perceived to have a principal objective of discouraging and deterring citizens,

including IT security experts, from investigating whether or not the personal information stored on the chip is secured against unauthorised changes. If it is not, the first people to find this out will be real criminals such as identity thieves etc. It has long been well known that security through obscurity in relation to information technology is completely ineffective.

53 Selling etc. your access card
You commit an offence if you sell, or otherwise transfer any part of your ownership of, your access card.
Penalty: Imprisonment for 10 years or 1,000 penalty units, or both.

The above new crime would give criminals who had stolen a card the opportunity to claim it was sold to them by the "owner", resulting in the owner in effect having to attempt to prove that they did not sell their card.

The pretence that individuals own the card should be dispensed with. All references to ownership by individuals, including the above new crime, should be deleted from the Bill.

54 Unlawful access cards
(1) The Secretary may require a person to give an access card to the Secretary if:
[... the Secretary suspects ...]
(3) A person commits an offence if:
...
(e) the person fails to give the access card to the Secretary immediately.

This offence enables the Secretary to demand a person surrender an access card merely on the basis that the Secretary suspects on reasonable grounds that it has either been obtained by means of false or misleading conduct or has been used in the commission of an offence against any law of an Australian jurisdiction.

The factual basis of the offence appears to be created by no more than the Secretary's suspicion, on reasonable grounds, of particular conduct by the card holder or another person. EFA considers this to be a completely inappropriate basis for a criminal offence of failing to give an access card to the Secretary immediately. The Secretary's suspicion may be wrong but nevertheless the person will not be able to access benefits or Medicare refunds after surrendering their card and may be subjected to considerable time and effort in attempting to obtain a replacement card. EFA questions what arrangements will be in place to ensure speedy replacement, at minimal inconvenience to the individual, of the card.

EFA also questions whether a person charged with such an offence will be sufficiently protected (or protected at all) by constraints on, and penalties for, any misuse of this power. We also observe that while the offence refers to the Secretary having such power, the power is also exercisable by any number of Commonwealth officers in participating agencies to whom the Secretary has delegated the power.

EFA also questions how it will be possible for a person to "give the access card to the Secretary immediately" especially in the case of persons located in remote areas where there are no DHS offices and hence no officer with delegated power to whom the card could be given "immediately".

Given the government claimed benefits of using a smart card, we would expect DHS to have in place appropriate systems for suspension and/or cancellation of suspect cards to prevent use of same for the purpose of obtaining government benefits whether or not a card is surrendered "immediately".

56 Possessing a false access card
(1) A person commits an offence if:
*(a) the person has possession or control of a *document; and*
*(b) the person knows that the document is a *false access card.*
Penalty: Imprisonment for 10 years or 1,000 penalty units, or both.
(2) Subsection (1) does not apply if the person has a reasonable excuse.
Note: The defendant bears an evidential burden in relation to the matter in subsection (2): see subsection 13.3(3) of the Criminal Code.

EFA notes the following extract from the Attorney-General's Department's *Guide to framing Commonwealth offences*[7]:

> "*Do not use 'without reasonable excuse'*
> *Principle: The phrases 'without reasonable excuse' or 'section X [being an offence] does not apply if the person has a reasonable excuse' should not be used in the context of Commonwealth offences.*
> *Discussion: These phrases are too open-ended and place uncertainty in the way of any prosecution as to what defence might be raised. Many of the exceptions to criminal responsibility thought to be caught by the "reasonable excuse" defence (such as duress, mistake or ignorance of fact, intervening conduct or event, and lawful authority) are covered by the generic defences in Part 2.3 of the Criminal Code. Either reliance should be placed on these defences, or additional specific defences should be set out.*
>
> *Generally, the only circumstance in which the use of a reasonable excuse defence can be justified is if the potential for innocuous conduct being caught by the offence is so great that it is not practical to design specific defences. In such cases there will be real questions about whether the width of the offence is too broad. Agencies wishing to include such defences in their legislative schemes should be asked to justify why they are needed. Often this process will force the agency sponsoring the legislation to articulate more clearly what they wanted the "reasonable excuse" defence to cover. This may lead to the development of more tailored/ specific defences, which is encouraged.*"

The fact that the phrase "without reasonable excuse" is used in the proposed offence shows that DHS knows that the width of the offence is too broad and believes that the potential for innocuous conduct to be caught by the offence is very great.

EFA submits that the offence should be re-drafted to significantly reduce the potential for innocuous conduct to be caught.

> *57 Unauthorised copying etc. of access card number, photograph or signature*
> *(1) A person commits an offence if:*
> *(a) the person does any of the following acts in relation to the* ***access card number, photograph or signature on the surface of an access card*** *:*
> *(i) copies or records it;*
> *(ii) keeps a copy or maintains a record of it;*
> *(iii) uses it in a manner connecting it with the identity of the owner of the access card;*
> *(iv) divulges or communicates it to a third person; and*
> *(b) the person is not the owner of the access card; and*
> *(c) either:*
> *(i) the person is not a *delegate or an *authorised person; or*
> *(ii) the person is a delegate or an authorised person but the person does not do the act for the purposes of this Act.*
> *Penalty: Imprisonment for 2 years or 120 penalty units, or both.*
> *(2) Subsection (1) does not apply if the owner of the access card consents in writing to the doing of the act.*
> *Note: The defendant bears an evidential burden in relation to the matter in 13 subsection (2): see subsection 13.3(3) of the Criminal Code. [emphasis added]*

EFA observes that changes to above offence since the exposure draft make it explicitly apply only to information *on the surface* of the card.

EFA submits that offences must also apply to copying etc. information stored in the chip in the card, and that it must apply to all information, not only the access card number, photo and signature.

We observe that the Explanatory Memorandum claims that:

> "*The consent will have to be in writing. Such consent will need to be obtained in a way that ensures that it is specific and informed consent. In accordance with the principle of informed consent, an individual can withdraw his or her consent.*"

However, the Bill itself does not state the above. Hence there is the distinct potential for "written consent" to be

obtained by burying a consent clause in a vast quantity of "fine print" on a form which an individual may be pressured into signing without having had an adequate opportunity to read all of it. The Bill should state that consent must be "specific and informed consent" and must require persons seeking such consent to specifically inform the person that he/she can withdraw consent in which case all previously copied information must be required to be promptly securely destroyed.

Further, EFA notes that the above section has undergone significant change since s270 of the exposure draft. While the changes have appropriately addressed some of the matters we raised in relation to s270 of the exposure draft, not all issues have been addressed. In our submission, we remarked:

> "The above offence [s270] appears to have been constructed without regard for the provisions of s190 which states 'You may use your access card for any lawful purpose you choose.'. If a person chooses to provide their access card to, for example, a bank for the purpose of opening an account, the bank is, we assume, required by other legislation to make a record of evidence of identity information. However, the above offence would appear to prevent them recording the number or making a photocopy of the card with the number printed on it.
>
> EFA agrees that it should be an offence to do the things in (a) above, but the offence should apply in the circumstance of doing so without the explicit and genuinely voluntary consent of the card holder. The proposed offence should be re-constructed accordingly. Such a construction should take care to deal appropriately with circumstances where a card holder is incapable of acting on their own behalf and another person is authorised to manage that person's personal affairs."

While the revised offence now enables copying etc with the written consent of the card "owner", it does not address the circumstances of persons who are incapable of acting on their own behalf.

62 Abuse of public office

This offence applies only to "a *delegate or an *authorised person" and only in the circumstance of dishonesty.

EFA questions what provisions/offences will be put in place to discourage and punish inappropriate browsing/viewing of information in the national ID database (Register) and disclosure of same by government agency staff and contractors.

The existing provisions of the *Privacy Act 1988* are inadequate in this regard as demonstrated by the decision in *NS v Commissioner, Department of Corrective Services [2004] NSWADT 263*[8]. Further information regarding the foregoing case and serious inadequacy of existing Commonwealth legislation is available in Section 5.1 of EFA's submission to the Inquiry into the Privacy Act 1988[9] conducted by the Senate Legal and Constitutional References Committee.

Division 7-Other offences
63 Protection of access card name and symbol
(1) A person commits an offence if the person, without the Minister's consent, does any of the following with a protected name or protected symbol:
(a) uses it in relation to a business, trade, profession or occupation; or
(b) uses it as the name, or as part of the name, of any firm, body corporate, institution, premises, vehicle, ship or craft
(including aircraft); or
(c) applies it, as a trade mark or otherwise, to goods imported, manufactured, produced, sold, offered for sale or let on hire; or
(d) uses it as part of a domain name; or

(e) uses it in relation to:
(i) goods or services; or
(ii) the promotion, by any means, of the supply or use of goods or services.
Penalty: 30 penalty units.
(2) In this section:

protected name means any of the following names:
(a) "Health and Social Services Access Card";
(b) a name determined under section 27 (whether or not the 24 determination remains in force); or a name so closely resembling a name in paragraph (a) or (b) as to be likely to be mistaken for it.

EFA welcomes the deletion of previous sub-section 1(e) (in the exposure draft) which would have prohibited use of a name, the same as or similar to the protected name, "as part of a URL". As pointed out in our submission on the exposure draft, such an offence:

> "would make criminals of individuals, organisations and businesses engaged in innocuous activity. For example an individual who used a URL like the following would commit an offence:
>
> http://www.examplemysite.id.au/Health and Social Services Access Card submission.pdf
>
> Similarly media organisations that produce URLs from article headings, whether by means of automated technology or not, would commit an offence with URLs such as:
>
> http://www.examplemediasite.com.au/news/company-wins-health-and-social-services-access-card-tender/2007/
>
> Use of the protected name in a URL would be prohibited by (1)(f) where use is in relation to goods and services and promotion thereof. No other use in URLs should be prohibited. Therefore 1(e) should be deleted [from the exposure draft]."

Accordingly, we hope such a provision does not re-appear in any amendments to the current Bill or a future Bill on the Access Card.

In relation to sub-section (2) above, we continue to be of the view that it should be limited to the actual name. If it is not so limited, then a significantly more certain definition of what is prohibited than "likely to be mistaken for it" (by who?) should be used in offence provisions.

Further, we observe that sub-section (2) has been amended to also apply to use of names that were in use by the government in the past. EFA questions how members of the public in the future will be able to know what name was referred to in determinations that were in force in the past. At the least, we consider there should be some limitation on the period for which a name remains protected after a determination ceases to be in force.

---

10. Civil Remedies Necessary

EFA is of the view that civil remedies, and possibly civil penalties, should be incorporated in the legislation.

We are concerned as to the probability of enforcement of a number of the criminal offences and hence whether these will afford adequate protection to individuals. This applies especially in relation to s45(2) as discussed earlier herein.

We are also doubtful about, for example, s57 in terms of the probability of prosecution being commenced against a person (e.g. doctors, chemists, etc) who divulges access card numbers in breach of that provision. In this regard, for example, the Australian Communications and Media Authority does not institute prosecution proceedings for breach of privacy protection provisions of the *Telecommunications Act 1997* where it considers that to enforce the law could disadvantage carriers and/or that only a small number of individuals' personal information has been unlawfully disclosed. Further, we note a recent case where the Federal Police were apparently not willing to prosecute in relation to unlawful disclosure of tax file numbers.

According to the decision in *H v Chartered Accountant [2006] PrivCmrA 7*[10], an accounting firm sent a list of TFNs of numerous employees of a company in liquidation to those employees, in error. Apparently the list was meant to be sent to the ATO. The decision states:

> "In the course of the investigation, the [Privacy] Commissioner formed the view that the disclosures might constitute a Tax File Number offence. The Commissioner advised the parties of this and referred the matter to the Australian Federal Police. The investigation was then discontinued but recommenced on advice from the

> Australian Federal Police that it would not institute proceedings for an offence in view of the nature of the alleged offence and its general impact."

(The outcome was that no sanction was applied to the accounting firm and no remedy was available to the complainant.)

That the Australian Federal Police decided not to institute proceedings is not, in our view, surprising given the Prosecution Policy of the Commonwealth[11]. This is not a criticism of that policy.

However, where individuals suffer detriment, disadvantage, inconvenience, costs, etc, arising from breach of the Act by another person, a combination of a decision not to prosecute and no civil remedy available will not be satisfactory.

Accordingly EFA submits that civil remedies should be provided to enable the Federal Court of Australia or a court of a State or Territory, on the application of an aggrieved person, to grant the aggrieved person remedial relief.

We consider remedial relief should be available to facilitate monetary compensation to persons for their time and related costs in obtaining a new Access Card (number) when, as one example, their card number has been disclosed in breach of the law. Civil remedies should also be available in circumstances such as where the Secretary (or a delegate) has required a card to be surrendered immediately and the Secretary's/delegate's suspicion was wrong.

---

11. Delegations and Authorisations

Division 3-Delegations and authorisations

EFA has not sufficient time to consider Part 5 Division 3 in detail. However, we have serious concerns about the breadth of, for example, the Secretary's authority to delegate powers to any Commonwealth officer in relation to, for example, power to form 'suspicion' and demand surrender of a card where failure to do so is a criminal offence. We consider legislation should narrowly restrict the number of officers to whom such powers are permitted to be delegated and ensure delegates may only be senior/high level officers.

---

12. Conclusion

As discussed above, the Bill contains many flaws and loopholes. Further, in the absence of the other two proposed tranches of Access Card legislation, and absence of publicly available detail concerning the architecture and operational aspects of the chip and system, it is impossible to know with any certainty the effect and potential ramifications of numerous provisions of the Bill.

Accordingly, EFA urges the Committee to recommend against enactment of the Bill. No Access Card legislation should be enacted until the government has publicly disclosed all details of the proposed system and the other two tranches of proposed legislation and there has been a significantly more appropriate length of time for public and Parliamentary scrutiny of such proposals than has been the case to date.

---

13. References

1. Human Services (Enhanced Service Delivery) Bill 2007.
<http://parlinfoweb.aph.gov.au/piweb/browse.aspx?path=Legislation%20%3E%20Current%20Bills%20by%20Title%20%3E%20Human%20Services%20(Enhanced%20Service%20Delivery)%20Bill%202007>

2. EFA submission to the DHS Access Card Consumer and Privacy Taskforce in response to Discussion Paper No. 1.
<http://www.efa.org.au/Publish/efasubm-dhs-accesscard-2006.html>

3. See Note 1.

4. Software House, FAQ about smart card readers
<http://readers.swhouse.com/pages/Smart_Card_Overview.aspx>

5. *Getting smart: the Access Card*, ABC Background Briefing, 28 Jan 2007.
<http://www.abc.net.au/rn/backgroundbriefing/stories/2007/1835583.htm>

6. Standing Committee on Finance and Public Administration, Estimates hearing, 16 February 2007.
<http://parlinfoweb.aph.gov.au/piweb/TranslateWIPILink.aspx?Folder=ESTIMATE&Criteria=DOC_DATE:2007-02-16

7. Attorney-General's Department's *Guide to framing Commonwealth offences, civil penalties and enforcement powers*, issued by authority of the Minister for Justice and Customs, February 2004.
<http://www.ag.gov.au/www/agd/agd.nsf/Page/Publications_FramingCommonwealthoffences,civilpenaltiesandenforce

8. *NS v Commissioner, Department of Corrective Services [2004] NSWADT 263*
<http://www.austlii.edu.au/cgi-bin/disp.pl/au/cases/nsw/NSWADT/2004/263.html>

9. Section 5.1 of EFA's submission to the Inquiry into the Privacy Act 1988
<http://www.efa.org.au/Publish/efasubm-slcrc-privact2004.html#52_22>

10. *H v Chartered Accountant [2006] PrivCmrA 7*
<http://www.austlii.edu.au//cgi-bin/disp.pl/au/cases/cth/PrivCmrA/2006/7.html>

11. Prosecution Policy of the Commonwealth
<http://www.cdpp.gov.au/Prosecutions/Policy/>

---

14. About EFA

Electronic Frontiers Australia Inc. ("EFA") is a non-profit national organisation representing Internet users concerned with on-line rights and freedoms. EFA was established in January 1994 and incorporated under the *Associations Incorporation Act* (S.A.) in May 1994.

EFA is independent of government and commerce, and is funded by membership subscriptions and donations from individuals and organisations with an altruistic interest in promoting online civil liberties. EFA members and supporters come from all parts of Australia and from diverse backgrounds.

Our major objectives are to protect and promote the civil liberties of users of computer based communications systems (such as the Internet) and of those affected by their use and to educate the community at large about the social, political and civil liberties issues involved in the use of computer based communications systems.

EFA policy formulation, decision making and oversight of organisational activities are the responsibility of the EFA Board of Management. The elected Board Members act in a voluntary capacity; they are not remunerated for time spent on EFA activities. The role of Executive Director was established in 1999 and reports to the Board.

EFA has long been an advocate for the privacy rights of users of the Internet and other telecommunications and computer based communication systems. EFA's Executive Director was an invited member of the Federal Privacy Commissioner's National Privacy Principles Guidelines Reference Group and the Research Reference Committee (2001) and the Privacy Consultative Group (2004-2005). EFA participated in NOIE's Privacy Impact Assessment Consultative Group relating to the development of a Commonwealth Government Authentication Framework (2003), Centrelink's Voice Authentication Initiative Privacy Impact Assessment Consultative Group (2004-2007), the ENUM Discussion Group and Privacy & Security Working Group convened by the Australian Communications and Media Authority ("ACMA" formerly ACA) (2003-2007), and the ACA's Consumer Consultative Forum meeting (April 2005). EFA has presented written and oral testimony to Federal Parliamentary Committee and government agency inquiries into privacy related matters, including amendments to the *Privacy Act 1988* to cover the private sector, telecommunications interception laws, cybercrime, spam, etc.
