Australian Government
Department of Foreign Affairs and Trade

Deputy Secretary

Telephone: 02 62613611
Facsimile: 02 62732081

8 March 2005

Ms Kelly Paxman
Acting Secretary
Senate Legal and Constitutional Committee
Parliament House
Canberra ACT 2600

Dear Ms Paxman

Inquiry into the *Privacy Act 1988*

Thank you for your letter dated 21 December 2004 to the Secretary of the Department of Foreign Affairs and Trade inviting a submission to the References Committee's Inquiry into the *Privacy Act 1988*. He has asked me to reply on his behalf.

Please find the Department's submission enclosed. This submission addresses two separate parts of the terms of reference relating to the overall effectiveness and appropriateness of the *Privacy Act 1988* as a means by which to protect the privacy of Australians. The submission covers the capacity of the current legislative regime to respond to the new and emerging technologies which have implications for privacy, including biometric imaging data. It also addresses any legislative changes that may help to provide more comprehensive protection or improve the current regime in any way, in the context of Australia's consular response to crises overseas.

Yours sincerely

(Gillian Bird)

SUBMISSION
BY THE DEPARTMENT OF FOREIGN AFFAIRS AND TRADE
TO THE SENATE LEGAL AND CONSTITUTIONAL COMMITTEE
INQUIRY INTO THE *PRIVACY ACT 1988*

The Department of Foreign Affairs and Trade (DFAT) welcomes the opportunity to provide a submission to the Senate Legal and Constitutional Committee Inquiry into the *Privacy Act 1988*. This submission addresses two separate parts of the terms of reference relating to the overall effectiveness and appropriateness of the *Privacy Act 1988* as a means by which to protect the privacy of Australians.

First, the submission addresses the capacity of the current legislative regime to respond to the new and emerging technologies which have implications for privacy, including biometric imaging data. Second, the submission addresses any legislative changes that may help to provide more comprehensive protection or improve the current privacy regime in any way, in the context of Australia's consular response to overseas crises involving Australians.

Facial biometric technology for ePassports

The ePassport project, for the introduction of facial biometric technology into Australian passports, is fundamentally about protecting the identities of Australians while meeting the needs of Australian travellers. It is as much about protecting the privacy of passport holders as it is about improving the security of the process.

The design of effective and appropriate privacy legislation has been a central consideration for the Government in implementing the ePassport project. A key element of the *Australian Passports Act 2005* is section 47 which regulates the use of technology for the purpose of confirming the validity of evidence of the identity of an applicant for an Australian passport or a person to whom an Australian passport has been issued. It is the Government's intention to implement the new Act in a manner consistent with the privacy principles and policies embodied in the *Privacy Act 1988*.

The four-year Biometrics Research and Development project has developed and identified technology which will ensure that the person holding a passport is the same person to whom that passport was issued. The information sought from applicants will remain the same as it has always been, that is a photograph. The only change is that the individual will be matched to an image of themselves by a machine rather than a person.

The Government has yet to approve the rollout of the ePassports project to full production. This is being considered as part of the normal budget process.

Proposed use of facial biometric technology

Facial biometric technology compares the unique facial features of each passport-holder to ensure that he or she is the person to whom the passport was issued, and that he or she is the same person who was issued with a previous passport with the same identity. Importantly, in the system under development, the information necessary for the creation of a person's biometric profile is obtained from the photograph of that

person provided with an ordinary passport application. Therefore, applicants will provide no more personal information than under the current system.

The use of facial biometric technology in producing and issuing an ePassport will occur in the following way.

First, the photograph of the applicant is digitised and converted to a machine readable form. It can then be compared with other photographs in the Australian passport database to prevent fraudulent applications. The software will do this by matching the applicants' images with their previous photographs and by confirming that the applicant has not previously applied in another (undisclosed) name.

Then, under the proposed system, the biometric information obtained from an individual's passport photograph will be stored in a contactless chip embedded in the passport.

Finally, the photograph is secured on the chip using Public Key Infrastructure. This technology is designed to verify the authenticity and integrity of the information stored on the contactless chip by the Australian Department of Foreign Affairs and Trade. In this way, border control authorities will be able to determine if the chip has been tampered with.

The "SmartGate" system at the Australian border will be able to match the information contained in the chip to the facial features and structure of the passport holder. In essence, this procedure merely substitutes the comparison between the photograph and the passport holder currently performed manually by Customs officials with a more reliable comparison conducted by electronic means. The only difference in the new system will be that the passport holder will be matched to an image of themselves by a machine rather than a person.

International Standards for Travel Documents

The introduction of biometric technology to Australian passports must comply with International Civil Aviation Authority (ICAO) Standards relating to the use of biometric technology in passports.

In 2003 the ICAO Technical Advisory Group on Machine Readable Travel Documents determined that facial recognition technology is the most effective means of machine-assisted identity confirmation. In May 2003 the Air Transport Committee of the ICAO Council adopted standards for the use of a 32K-minimum capacity contactless chip placed within the passport to store the biometric data. These specifications have the status of ICAO Standards.

Under the Convention on International Civil Aviation, Australia has an obligation to implement Standards adopted by ICAO. Under Article 37 of the Convention, Contracting Parties are obliged to "collaborate in securing the highest practicable degree of uniformity in regulations, standards, procedures and organization" in order to "facilitate and improve air navigation." Article 38 obliges Contracting Parties to notify ICAO of any differences between its own regulations or practices and the Standards promulgated by ICAO in the event that compliance is impracticable.

An increasing number of passport issuing authorities are moving to introduce biometric technology. These include the United States, the European Union, the United Kingdom, Japan, New Zealand, Canada, Italy, Ireland, Germany, Singapore and Hong Kong. This list includes many of the countries with which Australia shares a high volume of travellers.

Given this international uptake, introduction of this technology is necessary to meet the needs and expectations of Australian travellers.

For example, the introduction of biometric passports would enable the Government to ensure that the 300,000-plus Australian travellers to the USA each year would continue to enjoy the convenience of being part of the US Visa Waiver Program. Under the US Enhanced Border Security and Visa Entry Reform Act of 2002 (as amended), countries which wish to remain in the Visa Waiver Program are required to have introduced a biometric passports program by 26 October 2005. The US is introducing a biometric reading system, as part of "US-VISIT", at all its ports. Detailed information on the proposed use of this system is contained in Privacy Impact Assessments conducted by the US Department of Homeland Security.

For Australia, the US entry requirements merely place a practical deadline on a project that began in early 2000.

Some general privacy considerations relate to machine readable information, which will now include photographs, being made available to border control authorities in other countries. It is not practical to put in place enforceable controls on how that (freely available) information would then be used in another country. Moreover, whether a passport has a chip does not affect whether countries can electronically scan and store data page, including photograph information – some countries already do this by scanning the passport data page on arrival.

Australia is taking a leading role within ICAO's New Technology Working Group of the Technical Advisory Group to develop a normative annex to the MTRD blueprint which outlines best practice for the use of biometric data.

References to these documents are included at the end of this Submission.

Legislative regime for the use of facial biometric technology

The *Australian Passports Act 2005* is intended to come into force on 1 July 2005. Assuming the Government approves the full rollout of ePassports, it is envisaged that facial biometrics will be introduced into all Australian passports issued by 26 October 2005.

Section 47 of the Act will regulate the use of facial biometrics for the purposes of confirming the validity of evidence of the identity of an applicant for an Australian passport or a person to whom an Australian passport has been issued.

Section 47 contains several important safeguards to ensure that privacy principles are upheld and to protect against the misuse of personal information.

First, the determination made by the Minister for Foreign Affairs specifying the use of facial biometrics is subject to Parliamentary scrutiny, as it is a disallowable instrument.

In addition, as set out in the Note to subsection 47(1):

> *Any personal information collected as part of using a method specified in a determination must be dealt with in accordance with section 14 of the Privacy Act 1988 (including Information Privacy Principles 1 and 4).*

Information Privacy Principle 1 prohibits the collection of biometric information for passports by unfair or unlawful means, and prohibits its collection unless for purposes directly related to the passport operations of DFAT. These purposes have been codified in the new *Australian Passports Act 2005* (section 3). Information Privacy Principle 4 requires DFAT to securely protect biometric information provided to it by passport applicants and holders, and to do everything reasonable in the circumstances to prevent unauthorised disclosure of that information.

Finally, subsection 47(3) provides further privacy protection for individuals. It guards against the misuse of personal information, including biometric information, by requiring that any determination relating to the use of personal information must specify the nature of the personal information and the purposes for which it may be used. By imposing these requirements on the Minister, this provision ensures transparency in the way that biometric information may be used.

The Government considers that it is important for the community to be confident about the protection of their privacy while taking advantage of technologies (such as facial biometrics). The Government has conducted extensive consultation with travel, banking and technology industries; with the Federal Privacy Commissioner; and with privacy, human rights and consumer advocates. Key details of the new Act directly reflect their input. Moreover, the legislation as passed has incorporated suggestions made by the Opposition.

It is proposed that the Minister's determination will set out that the three separate uses of facial biometric technology, outlines above, in producing and issuing an ePassport. It will be underpinned by a Privacy Impact Assessment which will be subject to scrutiny by the Office of the Federal Privacy Commissioner (OFPC).

Consular Crisis Management Issues

In times of overseas crises involving Australians, DFAT's consular obligations and general responsibility to assist Australians overseas are triggered. To fulfil this role, the Australian community expects DFAT to make every effort to identify, locate and assist Australians in affected areas, particularly those persons directly affected by the crisis.

There have been three recent significant overseas crises involving Australians which have required a concerted consular response: September 11 (15,000 calls received resulting in 1500 persons unaccounted for); the Bali bombings (30,000 calls received resulting in 4500 persons unaccounted for) and the Boxing Day tsunamis (83,000 calls received resulting in 14,500 persons unaccounted for).

In administering the Government's response to these crises, DFAT has identified two key privacy-related impediments:

- DFAT's ability to access personal information held by other bodies to assist in its location, identification and assistance efforts; and
- DFAT's ability to provide personal information to other bodies directly involved in the crisis response.

In addition, DFAT has identified a related impediment regarding its ability to provide personal information to other bodies requesting the information to ensure inappropriate action is not taken against affected Australians.

DFAT access to personal information held by other bodies

To conduct a search for a large number of Australians in an overseas crisis situation and alleviate the anxiety of their family members and friends, DFAT needs to be able to verify quickly which persons reported as missing are likely to have been in the area affected by the crisis.

DFAT keeps an emergency database of persons reported as possibly affected or unaccounted for. This information is obtained from callers to the emergency hotline and from Australian consular officials in the affected countries. In the initial stages of this search, DFAT relies on checking these reports against information obtained from next-of-kin or emergency contacts listed in passport application forms and the Department of Immigration and Multicultural and Indigenous Affairs (DIMIA) arrival and departure information. In practice however, passport applications often do not contain up-to-date information and the next of kin or emergency contacts are not always aware of the passport holder's travel details.

DFAT needs to be able to reassure the community that it is doing everything it can to account for persons who may have been affected by the disaster. DFAT's response would be improved through access to personal information other government agencies hold which is more up-to-date and accurate than that currently available to DFAT. This would include, for example, up to date contact and next of kin details available from the Health Insurance Commission.

To meet our consular obligations, it would be useful to be able to access the records of airlines and travel agents regarding the travel plans, hotel reservations, and therefore general whereabouts, of Australians overseas. This information could, for example, confirm which Australians were booked in hotels directly affected by the Boxing Day tsunami. In response to inquiries, DFAT has been advised that airlines and travel agents are unable to disclose personal information because of restrictions in applicable privacy codes or the National Privacy Principles.

DFAT's ability to provide personal information to other agencies directly involved in the crisis response

DFAT needs to ensure that it is also able to provide promptly personal information to those other agencies that are directly involved in the Government's response to the overseas crisis.

Australians expect a seamless whole-of-government response to crises of this magnitude. While DFAT may be able to provide personal information to other agencies directly involved in the crisis response, for example, where there are reasonable grounds that the disclosure is necessary to prevent or lessen a serious or imminent threat to the life or health of the individual concerned, this is not necessarily applicable in all cases. For example, in the Boxing Day tsunami, the Department of Health and Ageing was keen to obtain information for State Health authorities which have responsibility for planning for Australians evacuated from affected regions. Although the Government agreed to evacuate affected Australians, not all cases could automatically be classified as "serious or imminent" threat to life or health. This example shows how DFAT's, and the Government's, ability to promptly and properly respond to the overseas crisis and best assist affected Australians could be impeded.

DFAT has been advised by the OFPC that, in some circumstances, DFAT's disclosure of personal information to bodies such as the AFP (to assist in the search and identification process) will be acceptable. However, the nature of the advice provided suggests that such disclosure may not always be possible, depending on the particular circumstances of the proposed disclosure. For example, mass casualty incidents overseas may or may not be the subject of an AFP investigation. Where they are not, valuable time can be lost while DFAT seeks advice on whether or not it can use Australian police expertise through their missing persons bureaux. The police can help identify those persons unaccounted for by confirming whether or not the person was in an affected area at the time, for example through analysis of bank and telephone records.

DFAT's ability to provide personal information to other agencies

Following the Bali bombing and Boxing Day tsunami, a number of bodies approached DFAT seeking information on persons hospitalised, persons for whom DFAT held grave concerns or persons unaccounted for. These agencies did not require the information as part of the Government's direct response to the overseas crisis, but to generally ensure that in the circumstances inappropriate action was not taken against affected Australians. For example, Centrelink wanted to avoid taking action to cancel regular social security payments to victims or pursuing persons affected by the tsunami for overdue payments.

Such requests were considered on a case-by-case basis and information was released where permissible under the Privacy Act. This process was time consuming, labour-intensive and, according to reports from interested bodies, impeded their ability to ensure that their Australian clients were not disadvantaged by being the victims of an international disaster.

The expectation of the Australian community is that there will be a whole-of-government response to the crisis and that government agencies are working collaboratively to achieve the best outcomes for affected Australians. Constraints under the Privacy Act limited DFAT's ability to provide personal information to some bodies that requested it, particularly those without specific information-gathering powers and State or Territory bodies. Except in a few cases, the Privacy Act does not allow DFAT to automatically share information on those persons affected or unaccounted for in an overseas disaster with other government agencies, which deliver services to these individuals.

References - Facial biometric technology for ePassports

ICAO TAG MRTD, "Biometrics Deployment of Machine Readable Travel Documents, Version 2.0, 5 May 2004.
Available through http://www.icao.int

ICAO Technical Action Group on Machine Readable Travel Documents (ICAO TAG MRTD), "Technical Report: PKI for Machine Readable Travel Documents offering ICC Read-Only Access", Version 1.1, 1 October 2004
Available through http://www.icao.int

ICAO New Technologies Working Group, "Proposed Amendments to ICAO Doc 9303 Part 1 to Accommodate the Biometrics Deployment Technical Report" Montreal 17 to 21 May 2004 (TAG-MRTD/15, WP/13).
Available through http://www.icao.int

ICAO Secretariat, "Biometric Technology in Machine Readable Travel Documents – The ICAO Blueprint", Twelfth Session of the Facilitation Division, Cairo, 22 March to 2 April 2004 (FAL/12-WP/4)
Available through http://www.icao.int

United States Department of Homeland Security (USDHS), "US-VISIT Program, Increment 1 Privacy Impact Assessment Executive Summary" 18 December 2003
Available through http://www.dhs.gov

USDHS, "US-VISIT Program, Increment 2 Privacy Impact Assessment" 14 September 2004
Available through http://www.dhs.gov

USDHS, "US-VISIT Program Privacy Policy" 14 September 2004.
Available through http://www.dhs.gov