Dear Mr Carter,
I have today sent by Express Post the OFPC's response to the question taken on notice at the 2 October hearing of the JCPAA inquiry into aviation security.

Attached for your convenience is an electronic copy of the letter, and one of the attachments. (The other attachment, being typographical corrections to Hansard, cannot be transmitted electronically.

Thank you for granting an extension for this information.

Best regards,

Hugh

Hugh Clapin
Deputy Director, Policy
Office of the Federal Privacy Commissioner
ph 02 9284 9759; fax 02 9284 9666

Or visit our website at: www.privacy.gov.au

Office of the Federal Privacy Commissioner

Framework for assessing and implementing new law enforcement and national security powers

The Office of the Federal Privacy Commissioner has developed a proposed framework for assessing and implementing new law enforcement and national security powers. The framework was first outlined in a paper for the Australian Institute of Criminology's conference in June 2001[1] and again in a submission to the Senate Legal and Constitutional Committee in April 2002 on proposed anti-terrorism legislation[2].

The framework sets out a life cycle approach to such proposals from development to implementation and review. The aim of the framework is to bring balance and perspective to the assessment of proposals for law enforcement or national security measures with significant effects on privacy.

First, careful analysis is needed in the development phase to ensure that the proposed measure is necessary, effective, proportional, the least privacy invasive option and consistent with community expectations. This analysis should involve consideration of the size, scope and likely longevity of the problem, as well as the range of possible solutions, including less privacy invasive alternatives. The impact on privacy of the

---

[1] 'Preserving Privacy in a rapidly changing environment' Paper presented to the Fourth National Outlook Symposium on Crime in Australia, New Crimes or New Responses convened by the Australian Institute of Criminology held in Canberra 21 June 2001

[2] Submission from the Federal Privacy Commissioner to the Senate Legal and Constitutional Legislation Committee Inquiry into Terrorism Bills April 2002

proposed solution should be analysed and critical consideration given to whether the measure is proportional to the risk.

Second, the authority by which the measure is implemented should be appropriate to its privacy implications. Where there is likely to be a significant impact on privacy, the power should be conferred expressly by statute subject to objective criteria. Generally, the authority to exercise intrusive powers should be dependent on special judicial authorisation. Intrusive activities should be authorised by an appropriately senior officer.

Third, implementation of the measure should be transparent and ensure accountability. Accountability processes should include independent complaint handling, monitoring, independent audit, and reporting and oversight powers commensurate with the intrusiveness of the measures.

Finally, there should be periodic appraisal of the measure to assess costs and benefits. Measures that are no longer necessary should be removed and unintended or undesirable consequences rectified. Mechanisms to ensure such periodic review should be built into the development of the measure. This could involve a sunset clause or parliamentary review after a fixed period.

In summary:

Analysis – is there a problem? Is the solution proportional to the problem? Is it the least privacy invasive solution to the problem? Is it in line with community expectations?

Authority – Under what circumstances will the organisation be able to exercise its powers and who will authorise their use?

Accountability – What are the safeguards? Who is auditing the system? How are complaints handled? Are the reporting mechanisms adequate? And how is the system working?

Appraisal – Are there built in review mechanisms? Has the measure delivered what it promised and at what cost and benefit?

OFPC 14 July 2003.

Our reference: 2003/0463/01km

Mr John Carter
Sectional Committee Secretary
Joint Committee of Public Accounts and Audit
Parliament House
Canberra ACT 2600

Dear Mr Carter

Matters taken on notice: JCPAA Inquiry into the Review of Aviation Security in Australia

I refer to matters taken on notice from my appearance on 2 October 2003 before the Committee in relation to its inquiry into the review of aviation security in Australia. I also attach some minor amendments to the Hansard of the Committee's public hearing (PA 79).

During the hearing, Senator Hogg asked, upon notice: (i) Since September 11, has the Office of the Federal Privacy Commissioner ('OFPC') provided advice to government, industry groups or unions about privacy issues surrounding security issues? (ii) If so, what was the nature of that advice?

(i) Advice to government, industry groups or unions about privacy issues surrounding security issues

The OFPC has provided advice to the following agencies in respect of this matter:

- Attorney-General's Department ('AGD');
- Australian Customs Service ('Customs');
- Department of Immigration and Multicultural and Indigenous Affairs ('DIMIA');
- Department of Foreign Affairs and Trade ('DFAT'); and
- Protective Security Coordination Centre ('PSCC').

The OFPC made submissions to the Senate Legal and Constitutional Legislation Committee in regard to the following:

- Inquiry into Terrorism Bills; and
- Inquiry into the Migration Legislation Amendment (Identification and Authentication) Bill 2003.

The OPFC provided advice to the Joint Committee on the National Crime Authority in relation to Australian Crime Commission Establishment Bill 2002.

No advice has been provided by the OFPC to industry groups or unions on this matter.

(ii) The nature of the advice

AGD

On 17 June 2003, the OFPC wrote to AGD in relation to proposed amendments to the *Australian Protective Services Act 1987*. The proposed amendments authorised Australian Protective Services officers, in defined circumstances, to collect personal information from an individual and to stop and search an individual.

OFPC's advice related to whether information collected under these provisions would form part of a permanent record or database, and the nature of the safeguards in place, including the provision notice to individuals in relation to the collection of their personal information.

Customs

Between 17 and 19 February 2003, the OFPC conducted an audit of Customs' Passenger Analysis Unit. The primary purpose of the audit was to ensure that Customs' new powers, to access advance passenger information (under the *Border Security Legislation Amendment Act 2002* and now section 64F of the *Customs Act 1901*) were being used in compliance with the Information Privacy Principles (IPPs) in the *Privacy Act 1988*.

The OFPC has provided Customs with a draft audit report and is currently considering Customs' response to this draft, before finalising the report.

The Office has also provided advice on Customs' facial recognition technology trial.

On 9 August 2002, OFPC sent a letter of advice to Customs regarding their proposal to trial SmartGate technology at Sydney airport. SmartGate uses facial recognition technology to scan a passenger's face and match it against his or her passport photograph.

In this letter, the OFPC outlined the relevant IPPs, and their relevance to the implementation of the trial, in particular IPP obligations relating to data retention.

DIMIA and the Senate Legal and Constitutional Legislation Committee

DIMIA consulted the OFPC on early drafts of the Migration Legislation Amendment (Identification and Authentication) Bill 2003.

The OFPC made a submission to the Senate Legal and Constitutional Legislation Committee's Inquiry into this Bill (available at the following URL: http://www.privacy.gov.au/publications/migsub.doc) .

The OFPC's advice to both DIMIA and the Senate Legal and Constitutional Legislation Committee, incorporated the OFPC's view on the importance of considering the 'AAAA' framework, (attached) when implementing measures to enhance security.

DFAT

On 15 July 2002, DFAT wrote to the OFPC seeking advice on its proposal to incorporate a biometric identifier in Australian passports. The proposal was to take an applicant's passport photo, transform it into an electronic portrait and check it against a database to ensure the applicant does not already have a passport. The electronic image was then to be stored on a computer chip in the passport and matched with a photograph taken of the traveller at Customs' checkpoints.

On 23 August 2002, the OFPC wrote to DFAT to offer advice on the proposal. The OFPC advised DFAT on the application of the relevant IPPs to the operation of the proposal, as well as providing general advice on the privacy issues involved. In particular, the advice reflected the OFPC's views on the importance of avoiding 'function creep' in the use of biometrics as identifiers.

PSCC

On 20 February 2003, the OFPC wrote to the PSCC to provide advice in relation to the National Security Hotline. The OFPC advised the PSCC on the application of the relevant IPPs to the operation of the National Security Hotline.

Senate Legal and Constitutional Legislation Committee's Inquiry into Terrorism Bills

The OFPC made a submission to this Inquiry (available at the following URL: http://www.privacy.gov.au/publications/secleg.doc).

The submission promoted the use of a framework to bring balance and perspective to the assessment of proposals for law enforcement or national security measures with significant effects on privacy. This framework has subsequently been distilled into the OFPC's 'AAAA' framework, which is recommended fro use in the development of similar policy proposals, and is attached for your information.

Joint Committee on the National Crime Authority

On 1 November 2002 the OFPC provided comments to the Joint Committee on the National Crime Authority in relation to the Australian Crime Commission Establishment Bill 2002 (available at the following URL: http://www.privacy.gov.au/publications/ncasub.pdf).

The submission drew attention to the need for appropriate oversight and accountability mechanisms in relation to the new body and its handling of personal information.

I hope that this information assists the Committee. Should you require further information, please contact Paul Armstrong (Director, Policy) on (02) 9284 9708, paul.armstrong@privacy.gov.au.

Yours Sincerely

Timothy Pilgrim

Timothy Pilgrim
Deputy Federal Privacy Commissioner

5 November 2003

Attachments:

- JCPAA Hansard for 2 October 2003, p. PA 79, with typographical amendments.
- Framework for Assessing and Implementing New Law Enforcement and National Security Powers (AAAA Framework).