

submission

Submission by Privacy NSW
on the proposed revision of the

Passports Act 1938 (Cth)



privacy**nsw**

Issue date: 1 April 2004

Privacy NSW Submission on the proposed revision of the Passports Act 1938 (Cth)

- **Introduction**

Privacy NSW is making this submission regarding proposed changes to the Passports Act 1938 (Cth) (the Act). Our comments are based on the information provided in a teleconference by Mr Adrian White of the Department of Foreign Affairs and Trade (DFAT) Passports Revision Group (PRG) and Mr Graham Austin, Acting Registrar of the New South Wales Registry of Births Deaths and Marriages (BDM). We have also based our comments on the information about the proposed changes to the Act in the Passports Revision Group Background Paper and other information on the DFAT Passports Australia website.

Our comments are in relation to:

- data exchanges between State and Commonwealth government
- the use of biometrics
- the use of unique identifiers
- the role of public consultation, and
- the need for a privacy impact assessment

Privacy NSW is the Office of the NSW Privacy Commissioner. The Privacy Commissioner is the holder of an independent statutory office, created by Parliament under the Privacy and Personal Information Protection Act 1998.

The functions of the Privacy Commissioner include making public statements about any matter relating to the privacy of individuals generally, and publishing reports and recommendations about any matter that concerns the need for, or the desirability of, legislative, administrative or other action in the interest of the privacy of individuals.

- The views in this paper

This submission reflects the views of the NSW Privacy Commissioner. It does not reflect the views of the NSW Government.

- **Data Exchanges between State and Commonwealth Agencies**

The Background Paper suggests that the new legislation will “set out clear provisions relating to exchanges of passport data” and that the primary purpose of this exchange would be to “verify information” provided by applicants and to “assist in establishing entitlement to a passport”. The Background Paper suggests that the flows of personal information would not just be from state agencies to DFAT, but also from DFAT to state agencies. Mr White advised that two NSW public sector information agencies (BDM and NSW Police) would be required to collect and disclose personal information. It

is not clear whether it is intended that the new legislation will permit information flows between DFAT and any other NSW public sector agencies or state owned corporations.

The collection and disclosure of personal information by NSW public sector agencies (as defined in the Privacy & Personal Information Protection Act 1998 (PPIP Act)) from DFAT is subject to restrictions imposed by the Information Protection Principles (IPPs) in Part 2 of the PPIP Act, unless provided for by an exemption in the Act.

BDM

We understand that DFAT proposes that the current Memorandum of Understanding (MOU) between DFAT and BDM¹ to provide DFAT with access to BDM's Certificate Validation Service Register is to be formalised in the new legislation. As we understand it, BDM checks the validity of birth, marriage and change of name certificates where those documents are relied upon by an applicant for a passport or other travel document .

This exchange of data between DFAT and BDM constitutes both a *collection* of personal information by BDM, and a subsequent *disclosure* of personal information back to DFAT.

In relation to BDM's obligations with respect to the collection of personal information, IPPs 1-4 require adherence to the following principles:

Lawful – only collect personal information for a lawful purpose. Only collect the information if it is directly related to the agency's activities and necessary for that purpose.

Direct – only collect information directly from the person concerned, unless they have given consent otherwise. Parents and guardians can give consent for minors.

Open – inform the person as to what information is being collected, why it is being collected and who will be storing and using it. Agencies must also inform the person how they can see and correct this information.

Relevant – ensure that the information is relevant, accurate, not excessive and up-to-date. Ensure that the collection does not unreasonably intrude into the personal affairs of the individual.

In terms of disclosure of personal information, BDM must comply with IPPs 11-12, which provide that disclosure must be:

Restricted – only disclose personal information if the person has given their consent or if they were informed at the time of collection that it would be disclosed in this way. You can only disclose the information for a related purpose if you believe the person concerned is not likely to object. Personal

¹ The MOU is dated 5 September 2001.

information can be disclosed without consent in order to deal with a serious and imminent threat to any person's health or safety.

Safeguarded – do not disclose sensitive personal information, for example, information about a person's ethnic or racial origin, political opinions, religious or philosophical beliefs, health or sexual activities or trade union membership. You can only disclose sensitive information without consent in order to deal with a serious and imminent threat to any person's health or safety

As we understand it, the main issue for BDM is whether BDM's collection of personal information from a third party (DFAT) and subsequent disclosure to a third party (new information back to DFAT) is authorised in the terms of the "consent" of the individual obtained by DFAT.

In relation to indirect collection, IPP 2 requires "authorisation" of the person. In terms of IPP 11 and 12, disclosure requires "express consent", which would appear to be a higher threshold than just "authorisation".

In a recent case brought before the Administrative Decisions Tribunal under the PPIP Act², the Tribunal reviewed the circumstances in which one NSW public sector agency collected personal information from another public sector agency. In that case, the disclosing agency relied upon the 'consent' obtained by the collecting agency to the data exchange. The Appeal Panel of the Tribunal found that this reliance did not constitute "express consent". The Appeal Panel held:

This legislation protects an aspect of an important human right, that of freedom from interference with privacy. The express consent provision should be strictly applied so as to underpin that right. In our view the requirement of express consent must be the subject of administrative action by the agency disclosing the information. It must have gone to the individual concerned and obtained an express consent that is precise as to the kind and, possibly, the exact contents of the information to which the consent relates [97].

A comprehensive summary of the case is attached as an appendix to this submission. Both the summary and the full text of the Appeal Panel's decision are available from Privacy NSW's website at:

<http://www.lawlink.nsw.gov.au/pc.nsf/pages/cases1>

As we understand it BDM are currently seeking legal advice on the application of this case to their current practices.

Our submission is that Commonwealth legislation should not seek to override the PPIP Act by diminishing the requirement for express consent to data exchanges between agencies.

² *Macquarie University v FM* [2003] NSWADTAP 43, see Appendix

NSW Police

We also understand that the new legislation would involve information flows between DFAT and NSW Police. We have been advised that NSW Police currently provide DFAT with information regarding warrants and other court orders which limit an individual's ability to travel, and that the new legislation will formalise this process. We understand that the PRG had yet to consult State and Territory Police but future consultation would take place through the Australian Federal Police.

NSW Police are required to comply with the IPPs in the PPIP Act in their exercise of their administrative and educative functions. Therefore disclosures of personal information by NSW Police for administrative purposes such as routine notifications of warrants and other court orders would be subject to the restriction on disclosure in IPPs 11-12 of the PPIP Act, as summarised above.

However, NSW Police need not comply with IPPs 11 and 12 if the disclosure is authorised by an exemption, such as section 23(5) and (7) of the PPIP Act which allows for disclosures for law enforcement purposes. Another exemption is found in section 25 of the PPIP Act which permits non-compliance if the agency is authorised, required or permitted by another law not to comply.

- **Facial Recognition Biometric**

The Background Paper states that the use of facial biometrics in passports "will assist in identifying fraudulent passport applications and detecting fraudulent use of a passport". We note that the Passports Australia 2002-03 Achievements and Challenges document found that over 500 cases of passport fraud were detected in 2001-02 and that the number of cases referred to the AFP for investigation increased by 6.6% in that year³. We acknowledge therefore that there is a need for increased passport security. As we understand it DFAT proposes to use a biometric identifier to detect and/or lessen the incidence of passport fraud. The Background Paper states that the new legislation will "set out the parameters" for the use of this biometric.

We expect that the Office of the Federal Privacy Commissioner will advise DFAT in greater detail about the legal and policy issues associated with the use of biometric identification. In particular, we draw your attention to a paper by the Federal Privacy Commissioner on how biometric technology can be used to deliver privacy-enhancing, rather than privacy-invasive, outcomes⁴.

- **Unique identifier**

We understand that the facial recognition biometric will involve the scanning of a hard-copy photograph, a process in which the image is translated into a

³ at page 21

⁴ http://www.privacy.gov.au/news/speeches/sp1_04_files/frame.html.

digital formula by the use of an algorithm, and the storage of information about the passport holder on a microchip (by way of the digital formula) which will be embedded into the passport. We understand that the algorithm will be encrypted and cannot be 'reverse engineered' to create a 'picture' of a person. We understand that when an individual presents at Australian or International Customs his or her face will be scanned and an algorithm which is created from the scanned image will be matched against the algorithm stored on the microchip in their passport. If there is a match the identity of the individual will have been verified. If there isn't a match it will be cause for further investigation as to whether the passport may have been fraudulently obtained.

The use of biometric identifiers, such as an algorithm created by facial scanning, creates a 'unique identifier'. An important protection for privacy is to ensure that the identifier is used for a specific purpose, and cannot be used for other transactions. One way to achieve this is through technology, another is through the law. We therefore suggest that the new legislation should limit the use of the algorithm or any other unique identifier generated as a result of biometric identifiers. For instance the legislation should establish strict controls for access to and use of the information, and require the production of a subpoena, warrant or other court order as a condition precedent to the disclosure of the information by DFAT.

- **Public Consultation**

The Background Paper states that public consultation "is important to ensure that the passport law meets the needs of the 8 million Australians who have a passport and the Australian community generally". Transparency about the use of personal information is an important dimension of privacy law and best practice, and Privacy NSW supports this statement. However we note that the Sydney and Melbourne public meetings to discuss the new changes were cancelled on the basis of low registration numbers. We are concerned that the uptake of the new passports may be negatively affected by the perception that the biometric and its associated uses will not be secure and will therefore represent a privacy risk.

We suggest that it is vital that there be broad-scale public consultation or at the very least a public awareness campaign to alert the general public to the future use of the biometric, and to the fact that penalties will be imposed on applicants who lose their passports on more than two occasions. Such consultation could form the basis for a more comprehensive privacy impact assessment which is discussed below.

- **Privacy Impact Assessment**

While we acknowledge that the PRG has limited time to prepare the draft legislation, we suggest that a privacy impact assessment is needed on the proposed changes not only to the legislation, but more critically, about the introduction of a biometric identifier in passports. A privacy impact assessment can provide "a credible source of information by assuaging

alarmist fears or alerting the complacent to potential pitfalls”⁵ and should be considered as part of an overall risk assessment process. In this case the rationale for undertaking a privacy impact assessment is to ensure the PRG has canvassed all the impacts that the proposed changes will have on individuals, and to address those impacts by various means. As a result of this process DFAT will have minimised the risk that the uptake of the new passports will be negatively affected.

A privacy impact assessment will enable an individual who will be affected by any new scheme which deals with their information to understand:

- What personal information the proposed scheme will deal with (in this case a photograph);
 - The sources from which this information is to be obtained (in this case the individual);
 - The circumstances in which collection is to take place (in this case when an individual applies for a passport for the first time or applies for the renewal of an existing passport);
 - The processing of that information (such as the collection of information from or disclosure to State and Territory agencies, and the means by which the photograph will be digitised and an algorithm created and encrypted);
 - The intended uses of the information (in this case for the purpose of verifying the identity of the individual); and
 - The safeguards against unauthorised access, use, disclosure, modification or loss (in this case the encryption of the algorithm and the legal requirements for securing the information and the prohibitions against access or secondary use).
- **Other matters for consideration**
1. It is not clear from the available documentation whether there will be a lead-in period for the introduction of the biometric, and if so, what the lead in time will be.
 2. The Background Paper states that the new legislation will exclude certain applicants who are “likely to engage in...specified serious crimes”. We suggest that where an agency intends to take administrative action against an individual, which might not only affect their access to the provision of services but might impinge of the presumption of innocence, that decision should not merely be based on the agency’s perception but on verifiable information such as a Police or other intelligence report. We submit that this should be reflected in the new legislation.

⁵ The New Zealand Privacy Commissioner’s Privacy Impact Assessment Handbook 2002 at point 4.

Appendix

Vice Chancellor, Macquarie University v FM

[2003] NSWADTAP 43
Date of decision: 23 September 2003

Case Note

This was an appeal against a finding by the Tribunal that two members of staff of Macquarie University had breached s18 of the PPIP Act by disclosing details of FM's conduct as a student at Macquarie to the University of New South Wales (FM v Macquarie University [2003] NSWADT 78). The information was disclosed during telephone conversations. There was no evidence that the information was previously written down or recorded in a material form by any staff member of Macquarie.

The decision of the Appeals Panel has important implications for the role of the Privacy Commissioner when appearing before the Tribunal. These implications will be incorporated into the Privacy Commissioner's proposed protocol for intervention in the Tribunal. The decision also provides significant guidance on the scope of the definition of personal information.

Role of Privacy Commissioner

In its appeal, Macquarie argued that the Tribunal had erred in allowing the Privacy Commissioner to make submissions under s55(7) of the *Privacy and Personal Information Protection Act 1998* (PIIP Act) without being joined as a party. Furthermore, Macquarie argued that the right of the Privacy Commissioner to appear and be heard was limited to proceedings at first instance and did not extend to proceedings at the Appeal Panel level. The Appeal Panel did not agree that the PIIP Act limits the right of the Privacy Commissioner as argued:

Section 55(7) should be given a construction which is consistent with the beneficial objects of this landmark piece of human rights legislation and the central role given to the Privacy Commissioner in the legislation to make it work. The Privacy Commissioner has an oversight role in relation to the way agencies handle complaints. There are many other powers and responsibilities given to the Privacy Commissioner by other parts of the Privacy Act of similar significance. It would make a mockery of these arrangements for the Privacy Commissioner to be cut out of the appeals environment of the Tribunal, where quite possibly some of the most significant questions touching on the scope and operation of the legislation might arise [41].

Definition of personal information

Macquarie argued that the meaning of personal information in s.4 of the PIIP Act is limited to information held in a material documentary form, for example, in paper records or electronic storage. Since the information disclosed to UNSW was merely held in the minds of the Macquarie staff members, Macquarie argued that such information was not subject to the IPPs. The Appeal Panel disagreed with Macquarie's arguments and found that:

there is nothing in our view in these exclusions [under s.4(3)] which could be said to read down the meaning of 'information' to that held in an agency in recorded or material form [71].

Macquarie also argued that the PPIP Act does not protect information in the nature of perceptions and knowledge that is obtained independently of university record keeping or collection of data by the University. The Appeal Panel did not accept that the meaning of "personal information" could be read down in this manner:

We see no reason in principle or in the terms of the words 'possession' or 'control' [in s.4(4)] to remove that kind of information from the sphere of protection given by the Privacy Act to individuals in this State who are the subject of comment by public sector agencies [78].

Requirements for "express consent"

The Appeal Panel considered whether the scope of an authorisation signed by FM when he enrolled at UNSW permitting UNSW to obtain "official records" from other tertiary institutions satisfied the requirement under s.26(2) for *express consent* to non-compliance with the restrictions on disclosure of personal information. The Appeal Panel held:

This legislation protects an aspect of an important human right, that of freedom from interference with privacy. The express consent provision should be strictly applied so as to underpin that right. In our view the requirement of express consent must be the subject of administrative action by the agency disclosing the information. It must have gone to the individual concerned and obtained an express consent that is precise as to the kind and, possibly, the exact contents of the information to which the consent relates [97].

Direction under s.41: Investigative Functions

Macquarie argued that the disclosure was permitted by the Direction on the Use of Information for Investigative Purposes made by the Privacy Commissioner under s.41 of the PPIP Act. The Tribunal initially held that the investigation conducted by UNSW was not a "lawful investigation" within the meaning of the direction. Accordingly, the Tribunal found that Macquarie could not rely on the Direction to the extent that it was carrying out an investigative function for UNSW.

On appeal Macquarie submitted that the UNSW conducted its investigation with the authority of statutory powers and common law. The Appeal Panel accepted this point and found that Macquarie was engaged in carrying out an investigative function in connection with the UNSW investigation.

The Appeal Panel delayed a final decision on whether the disclosure was permitted by the Direction because there had been no argument as to whether compliance might detrimentally affect the exercise of an agency's investigative functions as required by the Direction.

Scope of orders by Tribunal

Macquarie argued that the scope of the order made by the Tribunal under s.55(2)

was too broad in its application. The order required the Vice Chancellor and any person employed or engaged by Macquarie to restrain from disclosing information or opinions about students or former students unless an exemption under s18 applies.

The Appeal Panel agreed that it was generally more appropriate to make orders directed to the parties involved and based on the liability that has been established, rather than broad systemic orders covering the agency as a whole. Nevertheless the Appeal Panel noted, in the case of an inter partes order, that:

Obviously in well-administered organisations the order will be adopted as a precedent and a basis for policy that will govern all practice of a like kind [125].