



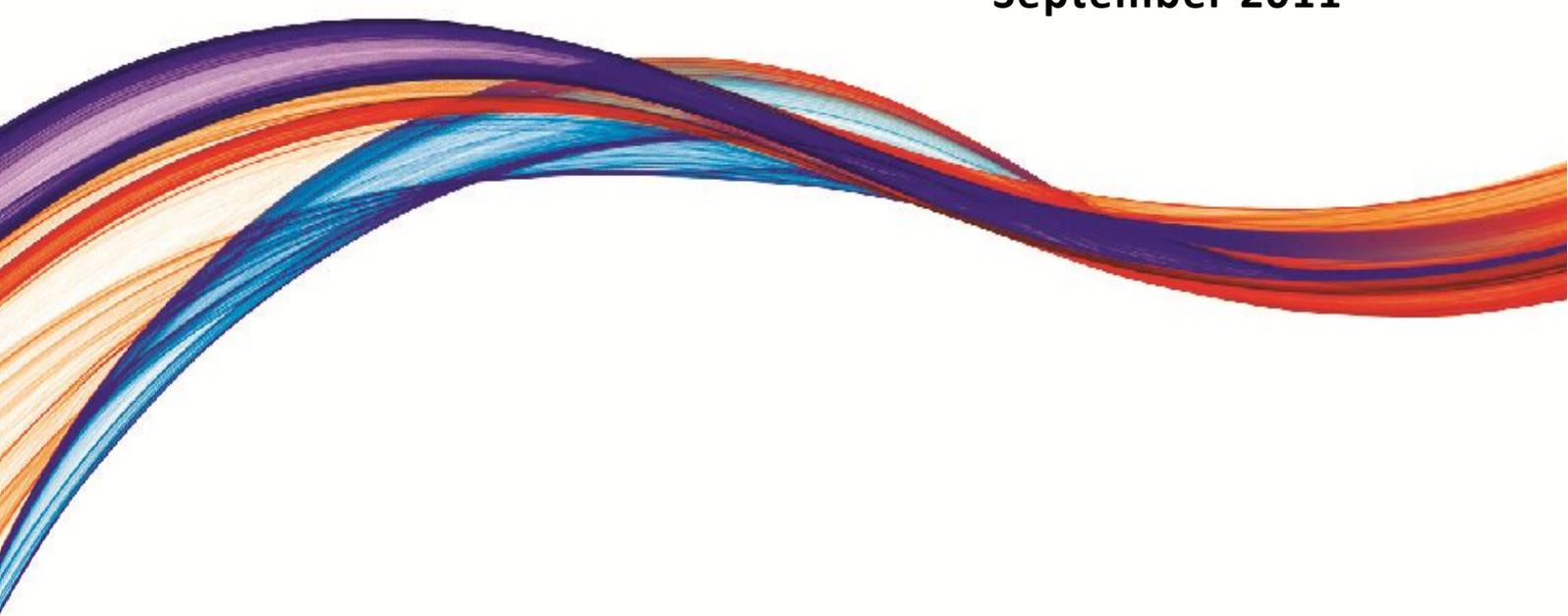
Australian Government

Office of the Australian Information Commissioner

Family Violence and Commonwealth Laws (DP 76)

**Submission to the Australian Law Reform
Commission**

September 2011



**Timothy Pilgrim
Australian Privacy Commissioner**

Introduction

The Office of the Australian Information Commissioner (the OAIC) was established by the *Australian Information Commissioner Act 2010* (Cth) (the AIC Act) and commenced operation on 1 November 2010.

The OAIC is an independent statutory agency headed by the Australian Information Commissioner. The Information Commissioner is supported by two other statutory officers: the Freedom of Information Commissioner and the Privacy Commissioner.

The former Office of the Privacy Commissioner (OPC) was integrated into the OAIC on 1 November 2010.

The OAIC brings together the functions of information policy and independent oversight of privacy protection and freedom of information (FOI) in one agency, to advance the development of consistent workable information policy across all Australian government agencies.

The Commissioners of the OAIC share two broad functions:

- the FOI functions, set out in s 8 of the AIC Act – providing access to information held by the Australian Government in accordance with the *Freedom of Information Act 1982* (Cth), and
- the privacy functions, set out in s 9 of the AIC Act – protecting the privacy of individuals in accordance with the *Privacy Act 1988* (Cth) (the Privacy Act) and other legislation.

The Information Commissioner also has the information commissioner functions, set out in s 7 of the AIC Act. Those comprise strategic functions relating to information management by the Australian Government.

In terms of the OAIC's privacy functions, the Privacy Act protects the 'personal information' of individuals handled by Australian Government agencies (as well as ACT and Norfolk Island agencies) and personal information held by all large private sector organisations, private health service providers and some small businesses. It does this through the application of binding privacy principles – the Information Privacy Principles (IPPs) generally apply to agencies, and the National Privacy Principles (NPPs) generally apply to organisations.

Comments on the Discussion Paper

The OAIC appreciates the opportunity to make comments to the Australian Law Reform Commission (the ALRC) on the Discussion Paper *Family Violence and Commonwealth Laws* (DP 76) (the Discussion Paper).¹ The OAIC previously provided comment on

¹ Discussion Paper available at: www.alrc.gov.au/publications/family-violence-and-commonwealth-laws-dp-76

Commonwealth legislative arrangements that impact on those experiencing family violence as part of its submissions on Issues Papers for this inquiry and refers you to its comments.²

The OAIC strongly supports initiatives to protect the safety of those experiencing family violence and to better support those adversely affected by this type of violence.

The OAIC recognises the sensitivity of personal information related to family violence matters and the potential for an individual to be stigmatised, embarrassed or discriminated against as a result of the disclosure or inappropriate sharing of this information. The challenge is to ensure that initiatives contain appropriate privacy safeguards regarding the handling of an individual's personal information, while providing strong protection against harm from family violence.

The right to privacy is not absolute and in some circumstances, privacy rights will necessarily give way where there is a compelling public interest reason to do so. In these instances, the OAIC seeks to ensure that the solution implemented minimises the intrusion to the fullest extent possible in the circumstances.

Screening, Information Sharing and Privacy

Proposal 4–13 *If a 'safety concern flag' is developed in accordance with Proposal 4–11, the Department of Human Services and other relevant departments and agencies should develop inter-agency protocols for information sharing between agencies in relation to the 'safety concern flag'. Parties to such protocols should receive regular and consistent training to ensure that the arrangements are effectively implemented.*

Proposal 4–14 *The Department of Human Services and other relevant departments and agencies should consider issues, including appropriate privacy safeguards, with respect to the personal information of individual customers who have disclosed family violence in the context of their information-sharing arrangements.*

The ALRC considers that a safety concern flag should be placed on a customer's file when safety concerns are raised, to provide the relevant agency staff member with an indication that the person may be eligible for different entitlements or exemptions, which in turn may ensure that their needs are responded to appropriately and ultimately may enhance their safety.³ It is further proposed that the existence of this flag could be shared between agencies, with the informed consent of the customer. The sharing of family violence information could ensure that victims do not have to repeat their story to different agencies and enable agencies to engage effectively with customers to provide appropriate services.⁴

In the context of information sharing between agencies, the OAIC is of the view that individuals should be given the opportunity to decide whether or not their personal

² Submissions made by the OAIC are available at: www.oaic.gov.au/publications/submissions.html#2011

³ Discussion Paper 76, paragraphs 4.3 and 4.111

⁴ Discussion Paper 76, paragraph 4.131

information will be shared not only between the Department of Human Services programs but also with other relevant departments. While personal information flows are central to service delivery, it is important for individuals to be able to exercise adequate choice and control over the way their information is handled. The OAIC would welcome an approach that places informed individual consent at the centre of any personal information sharing. Improving communication with customers as part of seeking informed consent may minimise the risk of misunderstandings about information sharing, which can lead to privacy complaints. It may also promote community trust and confidence in the handling of information by Australian Government agencies.

Privacy Impact Assessment

The OAIC strongly encourages a privacy impact assessment (PIA) be undertaken as part of developing protocols for the sharing of a 'safety concern flag' to ensure that any information sharing arrangement is in accordance with the Privacy Act and the Information Privacy Principles. In the context of undertaking a PIA for these information sharing arrangements, the OAIC considers that the PIA should also consider privacy obligations associated with the screening and subsequent collection and use of family violence information included in the safety concern flag.

A PIA is an assessment tool that describes in detail the personal information flows in a project. PIAs, updated at key stages of a project, can be an important tool in project risk management. The primary benefit of a PIA is that the identification and analysis of privacy impacts during the design phase can assist in determining the appropriate management of any potentially negative impacts. A project that underestimates privacy impacts can place its overall success at risk by not meeting the expectations of the community as to how personal information may be handled. PIAs are another aid to engendering community trust in new proposals.

Ideally, a PIA should be conducted by an independent expert in privacy and with experience in managing PIAs. The OAIC has a Privacy Impact Assessment Guide, providing an introduction to the PIA process.⁵ The Guide describes the purpose and general features of a PIA. The OAIC would welcome the opportunity to provide further advice and comment as part of the consultation process for a PIA.

Employment

Question 14–1 *In addition to removal of the employee records exemption in the Privacy Act 1988 (Cth), what reforms, if any, are needed to protect the personal information of employees who disclose family violence for the purposes of accessing new entitlements such as those proposed in Chapters 16 and 17?*

In *For Your Information: Australian Privacy Law and Practice*, (ALRC Report 108), the ALRC recommended the removal of the employee records exemption.⁶ In submissions to the inquiry that led to ALRC Report 108, the former OPC submitted that, on balance, given

⁵ Available at: www.oaic.gov.au/publications/guidelines/Privacy_Impact_Assessment_Guide.pdf

⁶ Recommendation 40-1

the desirability of national consistency of privacy regulation and to reflect community expectations, the employee records exemption provided in section 7B(3) of the Privacy Act should be removed. Reference was made to a number of benefits that may result from coverage of employee records under the Privacy Act, including being consistent with protection of an employee's rights as a private citizen, providing certainty about rights and obligations for employers and employees, eliminating regulatory difficulties in interpreting the exemption, and providing access to a conciliation-based complaints process through the Privacy Commissioner.⁷

Currently, where the disclosure of personal information to an employer is related to the employment of the employee, such as for the purposes of obtaining leave, it is personal information which constitutes an employee record. In the case of a private sector employer, the handling of employee records directly relating to the employment relationship is exempt in some circumstances from the operation of the Privacy Act.⁸

Generally, it is the view of the OAIC that there should be minimal exemptions from the Privacy Act to promote effective protection of privacy rights and reduce regulatory fragmentation. Where exemptions such as the employee records exemption currently exist there should be a sound public interest rationale for retaining them.

Employee records can contain a significant amount of personal information about employees. Furthermore, employers sometimes hold sensitive information, for example regarding the health or disabilities of their employees. Employees may be under economic pressure to provide this personal information to their employers for the purposes of accessing entitlements and have limited choice as to whether the information is provided. There is a real possibility of harm if employees' personal information is used or disclosed inappropriately. Where employers receive "sensitive" information, or information which due to its nature affected individuals may consider sensitive, such as evidence of family violence, employers should be required to handle that information in a manner consistent with the Privacy Act.⁹

The OAIC suggests that a number of benefits may result more generally from coverage of private sector employee records under the Privacy Act. Significantly these benefits may include:

- providing a minimum set of standards for privacy protection of employee records, consistent with protection of an employee's rights as a private citizen
- providing certainty about rights and obligations for employers and employees

⁷ Submission to the Australian Law Reform Commission's Review of Privacy - Issues Paper 31 (February 2007) chapter 5, paragraphs 104 – 113, available at: <http://www.privacy.gov.au/materials/types/download/9111/6748>; Submission to the Australian Law Reform Commission's Review of Privacy – Discussion Paper 72 (December 2007) chapter 36, available at: <http://www.privacy.gov.au/materials/types/submissions/view/6757>

⁸ Private organisations are exempt from the operation of the Privacy Act where an act or practice is directly related to: the employment relationship between the organisation and the individual; and an employee record held by the organisation. See Privacy Act ss 7(1)(ee), 7B(3).

⁹ Sensitive information is defined in s 6 of the Privacy Act.

- providing access to a conciliation-based complaints process through the OAIC.

While many private sector employers may already have adequate privacy policies and procedures in place for safeguarding personal information contained in employee records, the OAIC suggests that to realise the benefits of removing the exemption, additional guidance and information will be required for both employers and employees as to their respective obligations and rights.

Proposal 14–1 *There is a need to safeguard the personal information of employees who have disclosed family violence in the employment context. The Office of the Australian Information Commissioner and the Fair Work Ombudsman should, in consultation with unions and employer organisations:*

(a) develop a model privacy policy which incorporates consideration of family violence-related personal information; and

(b) develop or revise guidance for employers in relation to their privacy obligations where an employee discloses, or they are aware of, family violence.

The Australian Government has committed to considering whether the employee records exemption should be retained as part of the second stage response to ALRC Report 108.¹⁰ Were the Australian Government to remove the employee records exemption, the OAIC is supportive of the need to develop and publish guidance on the application of the Privacy Act to employee records, to assist employers in fulfilling their obligations.

In particular, the OAIC suggests that the guidance should aim to increase awareness about privacy issues relating to employee records. The guidance could usefully clarify how the Privacy Act applies to employers and interacts with the various requirements relating to the handling of personal information under the *Fair Work Act 2009* (Cth). Guidance materials could also encourage employers to develop policies and adopt practices aimed at safeguarding a person's privacy in the workplace.

In this context the OAIC considers that the more effective approach to assisting employers meet their obligations under the Privacy Act is the development of comprehensive guidance materials, rather than a model policy. Such an approach may assist employers in considering how they manage personal information in employee records and in the drafting of a privacy policy appropriate for their workplace. While it is acknowledged that the intent of a model policy is to provide a guide as to best practice, the availability of a model privacy policy may encourage organisations to adopt such a policy without consideration for the particular circumstances of that specific workplace.

The Pre-Employment Stage

Proposal 15–1 *Centrelink, DEEWR, JSA, DES and IEP providers, and ESAt and JCA assessors (through the Department of Human Services) should consider issues, including*

¹⁰ Australian Government, *First stage response to ALRC Privacy Report*, 2009, page 14 available at: www.dpmc.gov.au/privacy/reforms.cfm

appropriate privacy safeguards, with respect to the personal information of individual job seekers who have disclosed family violence in the context of their information-sharing arrangements.

This proposal raises similar issues to those considered earlier in response to proposals 4-13 and 4-14, and we refer to our comments on those proposals. The OAIC considers that the sharing of personal information about job seekers, including family violence information, between agencies and providers should generally occur with informed consent and in a manner consistent with Privacy Act obligations.

A balance must be struck between ensuring information is shared where it will assist the job seeker and the privacy risks associated with the sharing of personal information. The OAIC strongly encourages the undertaking of a PIA to assist in striking this balance. Undertaking a PIA may assist in the identification and analysis of privacy impacts and inform the consideration of appropriate privacy safeguards.

Superannuation Law

Question 19–16 *In practice, how do superannuation funds and APRA contact members or those who have made an application for early release of superannuation? Is there, or should there be, some mechanism or process in place in relation to applications involving family violence to deal with safety concerns associated with:*

(a) contacting the member or applicant; or

(b) the disclosure of information about the application?

The OAIC understands that in situations involving family violence, an applicant may make an application for early release of superannuation for the purposes of, preparing to leave a violent relationship. In such circumstances the ALRC suggests that the safety of the victim may be jeopardised by the manner in which the superannuation fund or APRA contacts the victim in relation to their application.¹¹

Security of personal information is a key element of privacy practice. The handling of personal information by APRA and superannuation funds is governed in part by the Privacy Act. The Privacy Act requires that both agencies and organisations ensure that reasonable steps are taken to protect personal information against loss, unauthorised access, modification or disclosure and other misuse.¹²

Generally, agencies and organisations will need to have a range of security safeguards in place to protect the personal information they hold. This includes protocols to address communication security, for example, policies and procedures that regulate how employees contact individuals via telephone or email to ensure that these communications are not intercepted by third parties. Additionally, it may be necessary to review employee training practices to ensure that all employees are aware of the

¹¹ Discussion Paper 76, paragraph 19.181

¹² Privacy Act, NPP 4 and IPP 4

protocols concerning leaving voice messages and email use. In reviewing existing processes the OAIC suggests consideration be given to undertaking a PIA to identify areas of privacy risk and to inform the development of mitigation strategies.