



Australian Government

Australian Law Reform Commission

Professor Rosalind Croucher  
President

Ms Natalya Wells  
Inquiry Secretary  
Standing Committee on Social Policy and Legal Affairs  
Department of the House of Representatives  
Parliament House  
Canberra  
ACT 2600

3 August 2012

Dear Ms Wells

### **Inquiry into the Privacy Amendment (Enhancing Privacy Protection) Bill 2012**

The Australian Law Reform Commission (ALRC) welcomes the release of the Privacy Amendment (Enhancing Privacy Protection) Bill 2012. As noted by the Attorney-General, the Hon Nicola Roxon MP, in her Second Reading Speech on the Bill, it implements some of the recommendations of the Australian Law Reform Commission (ALRC) in the 2008 report, *For Your Information—Australian Privacy Laws and Practice*, Report 108 (May 2008) (*For Your Information*). A copy of the report is available on the ALRC's website at [www.alrc.gov.au](http://www.alrc.gov.au), if further background information on the relevant recommendations would be of interest to the Committee.

The Committee invited submissions on four aspects of the Bill:

- (a) the adequacy of the proposed Australian Privacy Principles (APPs);
- (b) the efficacy of the proposed measures relating to credit reporting;
- (c) whether defences to contraventions should extend to inadvertent disclosures where systems incorporate appropriate protections; and
- (d) whether provisions relating to use of depersonalised data are appropriate.

The ALRC made submissions with respect to aspects of these reforms at other stages. First, there was the submission to the Senate Standing Committee on Finance and Public Administration in July 2010, with respect to the Australian Privacy Principles Exposure Draft and Companion Guide. Secondly, the ALRC made a submission in March 2011 to the Senate Finance and Public Administration Legislation Committee Inquiry into the Exposure Drafts of Australian Privacy Amendment Legislation, Part 2—Credit Reporting. Thirdly, the ALRC made a submission in October 2010 to the Standing Committee on Legal and Constitutional Affairs' inquiry into the Telecommunications Interception and Intelligence Services Legislation Amendment Bill 2010. A copy of each of these submissions is attached to this letter and forms part of the comments provided to the Standing Committee on Social Policy and Legal Affairs in the present inquiry. In this submission I provide some additional comments in relation to the APPs and the use of depersonalised data.

Australian Law Reform Commission  
Level 40, MLC Centre  
19 Martin Place, Sydney 2000

Postal Address:  
GPO Box 3708  
Sydney NSW 2001

Tel (02) 8238 6333  
Fax (02) 8238 6363

Web [www.alrc.gov.au](http://www.alrc.gov.au)  
Email [rosalind.croucher@alrc.gov.au](mailto:rosalind.croucher@alrc.gov.au)

### *Australian Privacy Principles*

I refer the Committee to the ALRC's submission on the APPs for general comment on the proposed principles—Attachment 1 to this letter. With respect to exemptions, the ALRC commented on a number of differences from the ALRC's recommendations—including in relation to missing persons, small businesses, registered political parties and employee records. The 2012 Bill includes additional matters to which I will refer.

#### *'Permitted general exceptions'*

Section 16A includes in table form those situations where the collection, use or disclosure of personal information is permitted by an 'APP entity' in the circumstances designated in the table. The inclusion in table form is consistent with Recommendation 33–1 of *For Your Information* that the exemptions for certain categories of agencies, organisations and entities or types of acts and practices be grouped together in a separate part of the Act and Recommendation 33–2 that exemptions for specific, named agencies, organisations and entities should be set out in a schedule.

The tabular form is a neat condensation of the core principles, but may need supporting information or notes, or a reconsideration of its location, to make it accessible to the general reader, as they sit apart from the Privacy Principles themselves. The ALRC recommended in Recommendation 18–1 that the privacy principles should be 'simple, clear and easy to understand and apply' and the presentation of the exemptions in s 16A, while the principles are in Schedule 1, may be at odds with this.

The ALRC advocated a two-pronged approach: that specific, named entities that are exempt from the Act should be set out in a schedule, clearly setting out the scope of any such exemption; and that exemptions for certain categories of entities or types of acts and practices should be grouped together. The object was to increase the accessibility and clarity of the exemption provisions. However the ALRC rejected the approach of locating exemptions within the principles themselves:

33.75 ... The alternative approach, of locating partial or full exemptions within specific privacy principles, has the potential to render the principles overly complex and unwieldy. Since all of the exemptions relate to specific functions or activities of an agency or organisation, rather than categories of information, locating exemptions within the definition of 'personal information' also would not be appropriate.

#### *Diplomatic and consular activities*

This is a new exception. The ALRC did not comment specifically about such a possible exception. If a comment were to be made about the proposed new exception it could be as to its scope, which is not particularly clear.

#### *Defence*

Item 7 of the table in s 16A refers expressly to defence. As the Explanatory Memorandum notes (at p 69), this is intended 'to clarify the circumstances where the collection of sensitive information may occur without consent outside Australia, and where personal information generally may be disclosed to an overseas recipient'.

Chapter 34 of *For Your Information* concerned intelligence and defence intelligence agencies. The ALRC concluded that the exemptions that applied to the intelligence and defence intelligence agencies under the *Privacy Act* should remain, as their central function was the covert collection and assessment of intelligence information. The ALRC rejected the approach advocated by some stakeholders that the intelligence and defence intelligence agencies should be subject to exceptions to specific privacy principles, rather than exempt from the operation of the *Privacy Act*.

34.109 ... All the intelligence and defence intelligence agencies already are subject to privacy rules or guidelines. The ALRC also is recommending that the ambit of these rules and guidelines be extended further to enhance privacy protection. In addition, the internal processes and methods of the intelligence and defence intelligence agencies are subject to a number of oversight and accountability mechanisms, including by the IGIS, the PJCIS and others. In particular, the IGIS has reported that he conducted regular inspections of the intelligence and defence intelligence agencies and actively monitored their adherence to privacy rules and guidelines. Finally, it should be noted that the OPC would have difficulties investigating or auditing the activities of the intelligence and defence intelligence agencies because it lacks the appropriate powers, infrastructure and security clearances to do so. For these reasons, it is not necessary to alter the scope of the exemption that applies to the intelligence and defence intelligence agencies under the *Privacy Act*.

The new exception is one for the ‘Defence force’, which is wider than the focus of the ALRC recommendations, and the activities described in Column 3 appear considerably broader than the covert intelligence-gathering context of the discussion in Chapter 34. I note further in this respect that ‘Defence force’ is defined in s 6(1) to include the Australian Navy Cadets, the Australian Army Cadets and the Australian Air Force Cadets, which opens the exception up far beyond the ALRC’s recommendations.

#### *Confidential alternative dispute resolution process*

Item 5 of the table in s 16A includes as a ‘permitted general situation’ the collection, use or disclosure of personal information where it is ‘reasonably necessary’ for the purposes of a confidential dispute resolution process. The ALRC recommended a similar exception: Recommendation 44–1. The key difference in the Bill is the inclusion of the word ‘reasonably’ to modify ‘necessary’. I note that the Explanatory Memorandum suggests that this is to be interpreted ‘objectively and in a practical sense’, but query whether it is necessary to shift the standard in this way.

#### *Defending legal or equitable claims*

Item 4 of the table in s 16A includes a similar provision in relation to the collection, use or disclosure of information where ‘reasonably necessary’ for the establishment, exercise or defence of a legal or equitable claim. In Chapter 44 of *For Your Information* the ALRC noted the ‘clear public policy interests in individuals being able to establish, pursue and defend legal rights’ and that one way of recognising this in the privacy context was through an exception to the ‘use and disclosure’ principle along the lines of s 35(2) of the *Data Protection Act* (UK). The ALRC concluded *against* making a recommendation of this kind.

44.45 It is not apparent, however, that adding an exception to this effect would substantially improve the position of intending litigants. To fulfil the requirements of the exception, an agency or organisation must be satisfied that disclosing the information is ‘necessary’ for the above purposes. This requirement will be very difficult to meet in the absence of a court order. Furthermore, the provision functions only as an exception to *permit* the disclosure of information—it does not compel disclosure by an agency or organisation.

44.46 The United Kingdom Information Commissioner’s Office has issued legal guidance on the Data Protection Act, which confirms that a data controller is not obliged to disclose personal data following a request by a third party, despite the existence of the exception for the purposes of establishing, exercising or defending legal rights. It advises:

In many cases, the data controller will not be in a position to make a decision as to whether the necessity test can be met, or will not wish to make the disclosure because of his relationship with the data subject, with the result that the requesting party will have to rely upon a Court order to obtain the information.

44.47 Processes are in place through court orders to obtain information in the course of establishing, exercising or defending legal rights. Court processes also have well established rules to prevent abuse by the parties. For example, an employer may request another organisation with which it has a business relationship to provide information on an employee’s purchasing activities to see if the employee is misappropriating funds. Without some evidence that misappropriation was, in fact, occurring, courts would consider this to be a ‘fishing expedition’ and, therefore, impermissible. This safeguard potentially could be bypassed through an exception to the ‘Use and Disclosure’ principle for the purpose of pursuing a legal claim.

44.48 Judicial discretion also plays an integral role in court orders for discovery against third parties. That is, for each application, the requirements of justice to the applicant will be balanced against the respondent's justification for non-disclosure. Commentators have noted that this discretion provides 'an appropriate brake on any excesses in the use of the Order'. Indeed, it has been questioned whether an agency should ever disclose personal information, except on the order of a court.

44.49 The ALRC acknowledges the potential drawbacks to requiring an individual to commence court proceedings in order to obtain personal information that he or she needs in order to establish, pursue or defend his or her legal rights. In particular—depending upon the court in which proceedings are commenced—this can be both costly and time-consuming. Court orders made in accordance with established rules, however, are the most authoritative way to secure disclosure. In light of the potential for abuse, as well as its likely limited usefulness, the ALRC does not recommend the introduction of a new exception or exemption from the *Privacy Act* for the purpose of establishing, pursuing and defending legal rights.

### *Use of depersonalised data*

The use of depersonalised data is a matter that is of particular utility in the context of research. The *Privacy Act* allows researchers to obtain and use personal information for health or medical research, without the consent of the individuals concerned, where approved by a Human Research Ethics Committee.

Chapter 65 of *For Your Information* focused on research and noted the concerns from researchers in the health and medical field—as well as social scientists, criminologists and others—that an overly cautious approach to the application of the *Privacy Act* was inhibiting the conduct of research, even where the threat to individual privacy was limited or non-existent and the potential value of the research was very high. For example, epidemiological research can play a very valuable role in planning and promoting public health campaigns and in allocating scarce resources. In such cases, researchers are not concerned with the identity or information of individuals within the sample, but rather are seeking to identify broad trends and patterns in the population.

The ALRC also recognised that there are other forms of research that provide benefits to the community that require access to personal information in situations where it is difficult to obtain consent—such as research on child protection or factors associated with criminal behaviour.

The ALRC recommended that the research exception to the 'Collection' and 'Use and Disclosure' principles should allow information to be collected, used and disclosed without consent for health and medical research—including in areas other than health and medical research—where a number of conditions were met, including approval by a Human Research Ethics Committee: Recommendations 65–2, 65–3, 65–4.

The Bill includes in s 16B 'permitted health situations' in relation to the collection, use or disclosure of health information. While badged in a different way, this provision is similar to existing provisions concerning the collection, use or disclosure of certain health information.

The ALRC recommended that the test for the research exception should be that Human Research Ethics Committees were satisfied that the public interest in the activity outweighs the public interest in maintaining the level of privacy protection under the *Privacy Act*: Recommendation 65–4. Such Ethics Committees work within the framework of guidelines under ss 95, 95A of the Act. One element is the weighing up of the public interest, which uses the modifier 'to a substantial degree' (s 95(2)) to maintain consistency with other parts of the Act.

While the research exception is one concerning situations of exception *from* the APPs, the ALRC's emphasis was upon ensuring appropriate levels of de-identification (or de-personalisation) of the relevant information:

65.163 It is appropriate to require agencies and organisations that have collected personal information for research purposes to take ‘reasonable steps’ to ensure that it is not possible to identify individuals from their published results. Reasonable steps might include, for example, applying techniques—employed by the ABS and other agencies ...—such as data suppression, data rounding and category collapsing. While these techniques minimise the risk that individuals will be identifiable, it is not always possible to ensure absolutely that no-one will be able to identify individual involved. In these circumstances, it would be inappropriate to impose absolute liability on agencies and organisations to ensure that information is not disclosed in an identifiable form.

65.164 It is also appropriate to impose a requirement that agencies and organisations ‘reasonably believe’ that the recipient of the personal information will not disclose the information in an identifiable form. Where agencies and organisations are not, themselves, in control of personal information because it has been disclosed to a researcher for use in a research project, for example, it is not possible for those agencies and organisations to ensure absolutely that the researcher will handle the information appropriately. On the other hand, the agency or organisation should be required to have a reasonable belief that this will occur. A ‘reasonable belief’ cannot be without foundation, and the agency or organisation would have to be able to indicate those factors that provided the basis for the belief—for example: the good reputation and past best practices of the researcher; and the arrangements put in place between the agency or organisation and the researcher to ensure that the information was handled appropriately.

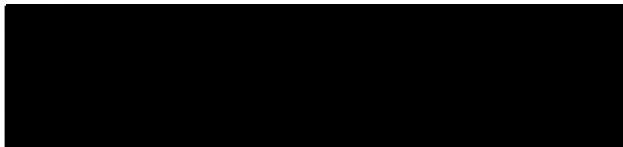
The ALRC recommended therefore in Recommendation 65–8 that the collection of personal information for research purposes should be permissible provided that, in addition to the matters broadly captured in s 16B of the Bill,

Where an agency or organisation collects personal information about an individual under this exception, it must take reasonable steps to ensure that the information is not disclosed in a form that would identify the individual or from which the individual would be reasonably identifiable.

While such matters may be covered in the Guidelines under ss 95 and 95A, given the importance of the provision as an *exception* to the APPs, an express statement about protection of information through de-identification may give the appropriate signal about the constraints on the use of the data.

I trust these brief remarks are of assistance to the Committee.

Sincerely,

A large black rectangular redaction box covering the signature area.

**Professor Rosalind Croucher**